KONICA MINOLTA

Giving Shape to Ideas

bizhub 754e/654e

User's Guide

Security Operations

2014. 11
Ver. 1.03

Contents

1 Security

1.1 Introduction ... 1-2
Compliance with the ISO15408 Standard ... 1-2
Operating Precautions ... 1-2
INSTALLATION CHECKLIST ... 1-3

1.2 Security Functions ... 1-5
Check Count Clear Conditions ... 1-5

1.3 Precautions for Operation Control ... 1-7
Roles of the Owner of the Machine ... 1-7
Roles and Requirements of the Administrator of the machine ... 1-7
Password Usage Requirements ... 1-7
User information control server control requirements ... 1-8
Security function operation setting operating requirements ... 1-8
Operation and control of the machine ... 1-8
Machine Maintenance Control ... 1-10

1.4 Miscellaneous ... 1-11
Password Rules ... 1-11
Precautions for Use of Various Types of Applications ... 1-12
Encrypting communications ... 1-12
Print functions ... 1-13
IPP printing ... 1-13
Items of Data Cleared by Overwrite All Data Function ... 1-14
Fax functions ... 1-14
USB keyboard ... 1-14
Different types of boxes ... 1-15
Hardware and software used in the machine ... 1-15
Firmware integrity verification function ... 1-15
IPsec setting ... 1-16
CS Remote Care function ... 1-16
Terminating a Session and Logging out ... 1-16
Authentication error during external server authentication ... 1-16

2 Administrator Operations

2.1 Accessing the Administrator Settings ... 2-2
2.1.1 Accessing the Administrator Settings ... 2-2
2.1.2 Accessing the User Mode ... 2-4

2.2 Enhancing the Security Function ... 2-8
2.2.1 Items cleared by HDD Format ... 2-10
2.2.2 Setting the Password Rules ... 2-11
2.2.3 Setting the Enhanced Security Mode ... 2-13

2.3 Preventing Unauthorized Access ... 2-16
Setting Prohibited Functions When Authentication Error ... 2-16

2.4 Canceling the Operation Prohibited State ... 2-18
Performing Release Setting ... 2-18

2.5 Setting the Authentication Method ... 2-20
2.5.1 Setting the Authentication Method ... 2-20
2.5.2 Setting the External Server ... 2-23

2.6 ID & Print Setting Function ... 2-26
Setting ID & Print ... 2-26

2.7 System Auto Reset Function ... 2-28
Setting the System Auto Reset function ... 2-28

2.8 User Setting Function ... 2-30
Making user setting ... 2-30

2.9 Account Track Setting Function ... 2-36
Making account setting ... 2-36
2.10 User Box Function ... 2-41
2.10.1 Setting the User Box ... 2-41
2.10.2 Changing the user/account attributes and box password ... 2-47
2.10.3 Setting Memory RX ... 2-52
2.11 Changing the Administrator Password ... 2-55
Changing the Administrator Password ... 2-55
2.12 Protecting Data in the HDD ... 2-58
2.12.1 Setting the Encryption Key (encryption word) ... 2-58
2.12.2 Changing the Encryption Key ... 2-62
2.12.3 Setting the Overwrite HDD Data ... 2-64
2.13 Overwrite All Data Function ... 2-66
Setting the Overwrite All Data function ... 2-66
2.14 Obtaining Job Log ... 2-68
2.14.1 Obtaining and deleting a Job Log ... 2-68
2.14.2 Downloading the Job Log data ... 2-70
Job Log data ... 2-72
2.15 Setting time/date in machine ... 2-79
2.15.1 Setting time/date ... 2-79
2.15.2 Setting daylight saving time ... 2-82
2.16 SSL Setting Function ... 2-84
2.16.1 Device Certificate Setting ... 2-84
2.16.2 SSL Setting ... 2-86
2.16.3 Removing a Certificate ... 2-87
2.17 S/MIME Communication Setting Function ... 2-88
2.17.1 Setting the S/MIME Communication ... 2-88
2.17.2 Registering the certificate ... 2-91
2.18 SNMP Setting Function ... 2-93
2.18.1 Changing the auth-password and priv-password ... 2-93
2.18.2 SNMP access authentication function ... 2-99
2.18.3 SNMP v3 setting function ... 2-99
2.18.4 SNMP network setting function ... 2-99
2.19 WebDAV Function ... 2-100
Setting the WebDAV Server Password ... 2-100
2.20 TCP/IP Setting Function ... 2-103
2.20.1 Setting the IP Address ... 2-103
2.20.2 Registering the DNS Server ... 2-104
2.21 AppleTalk Setting Function ... 2-105
Making the AppleTalk Setting ... 2-105
2.22 E-Mail Setting Function ... 2-106
Setting the SMTP Server (E-Mail Server) ... 2-106

3 User Operations

3.1 User Authentication Function ... 3-2
3.1.1 Performing user authentication ... 3-2
3.1.2 Accessing the ID & Print Document ... 3-8
3.2 Change Password Function ... 3-10
Performing Change Password ... 3-10
3.3 Secure Print Function ... 3-13
Accessing the Secure Print Document ... 3-13
3.4 User Box Function ... 3-17
3.4.1 Setting the User Box ... 3-17
3.4.2 Changing the user/account attributes and box password ... 3-23
3.4.3 Accessing the User Box and User Box file ... 3-30
3.4.4 Sending S/MIME box files ... 3-34

4 Application Software

4.1 PageScope Data Administrator 4-2
4.1.1 Accessing from PageScope Data Administrator 4-2
4.1.2 Setting the user authentication method 4-5
4.1.3 Changing the authentication mode 4-7
4.1.4 Making the user settings 4-10
4.1.5 Making the account settings 4-11
4.1.6 Registering the certificate 4-12
4.1.7 DNS Server Setting Function 4-14
4.1.8 AppleTalk Setting Function 4-15
4.1.9 E-Mail Setting Function 4-16

1 Security

1 Security

1.1 Introduction

Thank you for purchasing our product.

This User's Guide contains the operating procedures and precautions to be used when using the security functions offered by the bizhub 754e/654e machine. To ensure the best possible performance and effective use of the machine, read this manual thoroughly before using the security functions. The administrator of the machine should keep this manual for ready reference. The manual should be of great help in finding solutions to operating problems and questions.

This User's Guide (version 1.03) covers the following.

Model name	bizhub 754e/bizhub 654e/ineo 754e/ineo 654e
Version	G00-60

For any query, request, or opinion concerning the machine, please contact your dealer from which you purchased your machine or Service Representative.
Any notice concerning this machine will be given in writing by the dealer from which you purchased your machine or Service Representative.

Compliance with the ISO15408 Standard

When the Enhanced Security Mode on this machine is set to [ON], more enhanced security functions are available.

This machine offers the security functions that comply with the ISO/IEC15408 (level: EAL3) and IEEE Std 2600.1-2009.

Operating Precautions

The machine gives an alarm message or an alarm sound (peep) when a wrong operation is performed or a wrong entry is made during operation of the machine. (No "peep" alarm sound is issued if a specific sound setting in Sound Setting of Accessibility Setting is set to [OFF].) If the alarm message or alarm sound is given, perform the correct operation or make the correct entry according to the instructions given by the message or other means.

The administrator of the machine should exit from the current mode to return to the basic screen whenever the access to that mode is completed or if he or she leaves the machine with the mode screen left displayed.

The administrator of the machine should make sure that each individual general user exits from the current mode to return to the basic screen whenever the access to that mode is completed or if the user leaves the machine with the mode screen left displayed.

If an error message appears during operation of the machine, perform steps as instructed by the message. For details of the error messages, refer to the User’s Guide furnished with the machine. If the error cannot be remedied, contact your service representative.

The PageScope Web Connection functions can be used only if the setting is made to accept "Cookie."

INSTALLATION CHECKLIST

This Installation Checklist contains items that are to be check by the Service Engineer installing this machine. The Service Engineer should check the following items, then explain each checked item to the administrator of the machine.

To Service Engineer

Make sure that each of these items is properly carried out by checking the box on the right of each item.

1.	Perform the following steps before installing this machine.	
	Check with the administrator to determine if the security functions of this machine should be enhanced. If the functions should be enhanced, check the following. If the security functions are not to be enhanced, quit the operation without checking the following.	☐
	Before installing the machine, check with the administrator of the machine to determine if the following is confirmed. • Whether the Service Engineer has been informed that the unpacking procedure is to be performed by the Service Engineer in the presence of the administrator of the machine. • Whether the machine has been under the control of the administrator of the machine with a check made to ensure that evidently the machine has not been unpacked or used. The Service Engineer should obtain the administrator's consent to the performance of this item. If the machine has been unpacked, check with the administrator that it was the administrator who unpacked the machine and nobody but the administrator has gain access to the machine after the unpacking. Then, obtain the administrator's consent to the performance of the installation procedure for the unpacked machine before attempting to start the procedure. If the administrator's consent cannot be obtained, call the dealer.	☐
	I swear that I would never disclose information as it relates to the settings of this machine to anybody, or perform malicious or intentional act during setup and service procedures for the machine.	☐
	When giving a copy of the User's Guide, explain the following to the administrator: • A digital signature is assigned to the data certified by ISO15408. To ensure integrity of the file, have the administrator of the machine confirm the digital signature using the property of the provided data file in the user's PC environment. • Two versions are available, the HTML version and User's Guide Security Operations (this User's Guide). • This User's Guide must first be read and the conditions described in this User's Guide take precedence over the HTML version. • If the security functions of the machine are to be enhanced, the machine and its surrounding environment should be set up and operated according to this User's Guide.	☐
	Refer to the Service Manual and perform the required installation and setup steps. During the installation and setup procedure, make sure that no unnecessary parts are mounted on the machine and have the administrator of the machine confirm that no unnecessary parts are mounted on the machine.	☐
2.	After this machine is installed, refer to the Service Manual and perform the following steps.	
	Check that the SSD mounted on the machine is the type for the exclusive use for this machine.	☐
	Check that the Fax Kit has been mounted and set up properly, if fax functions are to be used. After the installation, conduct transmission and reception tests to make sure that the Fax Kit has been mounted and set up properly.	☐
	Let the machine read the Custom Function Pattern Selection setting file XXX_v1.0_ISO15408.cpd.	☐
	Get the administrator of the machine to confirm that [ISO15408] is selected for [Send/Save] of [Custom Function Pattern Selection] in the Administrator Settings and obtain his or her consent not to change the setting.	☐

	Check that the model name and the Firmware version (card version, BOOT) checked with the Service Manual agree with the value shown on the Firmware version display screen. Check also that the MFP model name and the part numbers of the MFP board and the SSD board agree with those described in the Service Manual. If there is a mismatch in the Firmware version number, explain to the administrator of the machine that upgrading of the Firmware is necessary and perform upgrading of the Firmware.	☐
	Set CE Authentication to [ON] and set the CE Password.	☐
	Make the service settings necessary for the Enhanced Security Mode.	☐
3.	After this machine is installed, refer to this User's Guide and perform the following steps.	
	Check that the Administrator Password has been set by the administrator of the machine.	☐
	Check that the Encryption Key has been set by the administrator of the machine.	☐
	Check that the Overwrite HDD Data has been set by the administrator of the machine.	☐
	Check that User Authentication has been set to [ON (MFP)] or [External Server Authentication] (Active Directory only) by the administrator of the machine.	☐
	Check that the self-signed certificate for SSL communications has been registered by the administrator of the machine.	☐
	Check that the Job Log Settings (Audit Log) has been set by the administrator of the machine.	☐
	Check that the date and time have been correctly set in the machine by the administrator of the machine.	☐
	Check that the ID & Print has been set by the administrator of the machine.	☐
	Check that the Memory RX has been set by the administrator of the machine.	☐
	Check that the S/MIME Communication has been set by the administrator of the machine.	☐
	Check that IPsec has been set by the administrator of the machine for communications between the machine and the DNS server.	☐
	Check that IPsec has been set by the administrator of the machine for communications between the machine and the SMTP server.	☐
	Check that the various functions to be disabled manually have been properly disabled by the administrator of the machine.	☐
	Let the administrator of the machine set Enhanced Security Mode to [ON].	☐
	The languages, in which the contents of the User's Guide Security Operations have been evaluated, are Japanese and English. The following lists the manuals compatible with bizhub 754e/bizhub 654e/ineo 754e/ineo 654e (Version: G00-60). • bizhub 754e/654e User's Guide v1.00 A55V-9607BA-00 • bizhub 754e/654e User's Guide Security Operations 2014. 11 Ver. 1.03	☐
	Explain to the administrator that the settings for the security functions for this machine have been specified.	☐

When the above steps have been properly carried out, the Service Engineer should make a copy of this page and give the original of this page to the administrator of the machine. The copy should be kept at the corresponding Service Representative for filing.

Please direct your any queries about using the machine to the Service Representative shown below.

Product Name		Company Name	User Division Name, Contact	Person in charge
Customer (administrator of machine)				
Service Representative				

1.2 Security Functions

Setting the Enhanced Security Mode to [ON] will validate the security function of this machine. For details of the settings of different security functions to be changed by turning [ON] the Enhanced Security Mode, see page 2-8.

The following the major security functions when the Enhanced Security Mode is set to [ON].

Function	Description
Identification and authentication function	Access control is then provided through password authentication for any access to the Administrator Settings, User Authentication mode, User Box, a User Box data file, a Secure Print document, SNMP authentication, and WebDAV server. Access is thereby granted only to the authenticated user. A password that can be set must meet the Password Rules. The machine does not accept setting of an easily decipherable password. For details of the Password Rules, see page 1-11. If a wrong password is entered, during password authentication, a predetermined number of times (once to three times. twice, four times, or six times for the WebDAV Server Password) or more set by the administrator of the machine, the machine determines that it is unauthorized access through Prohibited Functions When Authentication Error, prohibiting any further entry of the password. By prohibiting the password entry operation, the machine prevents unauthorized use or removal of data. The administrator of the machine is responsible for resetting the prohibition of the password entry operation. For details, see page 2-18.
User limiting function	Specific functions to be used by each user/account may be limited. For details, see page 2-30.
HDD encryption function	By setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. For details, see page 2-58.
Auditing function	Information including operations performed on the machine and a job history can be stored in the HDD. Setting the Job Log (Audit Log) allows an illegal act or inadequate operation performed on the machine to be traced. The obtained Job Log can be downloaded and viewed from the PageScope Web Connection. For details, see page 2-68.
Residual information deleting function	When the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, setting of the Overwrite HDD Data function while the machine was in use allows residual unnecessary data to be deleted, because the machine overwrites a specific overwrite value over the unnecessary data. This prevents data leakage. (Passwords, addresses, and other data set while the machine was in use should, however, be deleted manually.) For details, see page 2-64. To delete data including the passwords, addresses, and other data all at once, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the memory area on the MFP board and the SSD board to factory settings, preventing data from leaking. For details, see page 2-66. For details of items to be cleared by Overwrite All Data function, see page 1-14.
Network communication protecting function	Communication data transmitted to or from the machine and client PC can be encrypted using the SSL/TLS, which prevents information leakage through sniffing over the network. For details, see page 2-84.

Check Count Clear Conditions

The following are the conditions for clearing or resetting the check count of the number of wrong entries at the time of authentication by the Enhanced Security Mode.

<Administrator Settings>

- Authentication of Administrator Settings is successful.

<User Authentication Mode>

- User Authentication mode is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<Account Track Mode>

- Account Track mode is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<Secure Print>

- Authentication of Secure Print is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<Box>

- Authentication of User Box is successful.
- Authentication for execution of change of User Box Name and User Box Password is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<SNMP Password (auth-Password, priv-Password)>

- Authentication of SNMP is successful.
- Release of Prohibited Functions When Authentication Error is executed.

<WebDAV server password>

- Authentication of WebDAV server is successful.
- Release of Prohibited Functions When Authentication Error is executed.

1.3 Precautions for Operation Control

This machine and the data handled by this machine should be used in an office environment that meets the following conditions. The machine must be controlled for its operation under the following conditions to protect the data that should be protected.

Roles of the Owner of the Machine

The owner (an individual or an organization) of the machine should take full responsibility for controlling the machine, thereby ensuring that no improper operations are performed.

- The owner of the machine should have the administrator of the machine recognize the organizational security policy and procedure, educate him or her to comply with the guidance and documents prepared by the manufacturer, and allow time for him or her to acquire required ability. The owner of the machine should also operate and manage the machine so that the administrator of the machine can configure and operate the machine appropriately according to the policy and procedure.
- The owner of the machine should have users of the machine recognize the organizational security policy and procedure, educate them to follow the policy and procedure, and operate and manage the machine so that the users acquire the required ability.
- The owner of the machine should vest the user with authority to use the machine according to the organizational security policy and procedure.
- The owner of the machine should operate and manage the machine so that the administrator of the machine checks the Job Log (Audit Log) data at appropriate timing to thereby determine whether a security compromise or a faulty condition has occurred during an operating period.
- If the Job Log (Audit Log) data is to be exported to another product, the owner of the machine should ensure that only the administrator of the machine performs the task. The owner of the machine should also operate and manage the machine so that the Job Log (Audit Log) data is not illegally accessed, deleted, or altered.

Roles and Requirements of the Administrator of the machine

The administrator of the machine should take full responsibility for controlling the machine, thereby ensuring that no improper operations are performed.

- A person who is capable of taking full responsibility for controlling the machine should be appointed as the administrator of the machine to make sure that no improper operations are performed.
- When using an SMTP server (mail server) or an DNS server, each server should be appropriately managed by the administrator and should be periodically checked to confirm that settings have not been changed without permission.

Password Usage Requirements

The administrator must control the Administrator Password, Encryption Key, auth-password, priv-Password, and WebDAV Server Password appropriately so that they may not be leaked. These passwords should not be ones that can be easily guessed. The user, on the other hand, should control the User Box Password, Secure Print Password, and User Password appropriately so that they may not be leaked. Again, these passwords should not be ones that can be easily guessed. For the Public User Box shared among a number of users, the User Box Password should be appropriately controlled so that it may not be leaked to anyone who is not the user of the Public User Box.

<To Achieve Effective Security>

- Make absolutely sure that only the administrator knows the Administrator Password, Encryption Key, auth-password, priv-Password, and WebDAV Server Password.
- The administrator must change the Administrator Password, Encryption Key, auth-password, priv-Password, and WebDAV Server Password at regular intervals.
- The administrator should make sure that any number that can easily be guessed from birthdays, employee identification numbers, and the like is not set for the Administrator Password, Account Password, Encryption Key, auth-password, priv-Password, and WebDAV Server Password.
- If a User Password or User Box Password has been changed, the administrator should have the corresponding user change the password as soon as possible.
- The administrator should change the Account Password set for each account at regular intervals and, should one be changed, he or she should immediately inform users who implement Account Track of the new Account Password.
- If the Administrator Password has been changed by the Service Engineer, the administrator should change the Administrator Password as soon as possible.

- The administrator should have users ensure that the passwords set for the User Authentication, Secure Print, and User Box are known only by the user concerned.
- The administrator should have users who implement Account Authentication ensure that the Account Password set for the account is known by the users implementing Account Authentication only.
- The administrator should make sure that only the users who share a Public User Box and Group User Box know the password set for it.
- The administrator should have users change the passwords set for the User Authentication and User Box at regular intervals.
- The administrator should make sure that any user does not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the passwords set for the User Authentication, Secure Print, and User Box.

User information control server control requirements

For the user information control server connected to the LAN within the office, in which this machine is installed, the server administrator is required to apply patches and register only users who are authorized to use the machine.

Security function operation setting operating requirements

The administrator of the machine should observe the following operating conditions.

- The administrator of the machine should make sure that the machine is operated with the settings described in the installation checklist made properly in advance.
- The administrator of the machine should make sure of correct operation control so that the machine is used with the Enhanced Security Mode set to [ON].
- When the Enhanced Security Mode is turned [OFF], the administrator of the machine is to make various settings according to the installation checklist and then set the Enhanced Security Mode to [ON] again. For details of settings made by the service engineer, contact your service representative.
- When the machine is to be discarded or use of a leased machine is terminated at the end of the leasing contract, the administrator of the machine should use the Overwrite HDD Data function and the Overwrite All Data function to thereby prevent data to be protected from leaking.

Operation and control of the machine

The administrator of the machine should perform the following operation control.

- The administrator of the machine should log off from the Administrator Settings whenever the operation in the Administrator Settings is completed. The administrator of the machine should also make sure that each individual user logs off from the User Authentication mode after the operation in the User Authentication mode is completed, including operation of the Secure Print document, User Box, and User Box file.
- During user registration and box registration, the administrator of the machine should make sure that the correct settings are made for the correct users, including functional restrictions and box attributes.
- The administrator of the machine should set the Encryption Key according to the environment, in which this machine is used.
- The administrator of the machine should appropriately control the device certificate (SSL certificate) registered in the machine.
- The administrator of the machine should ensure that no illegal connection or access is attempted when the machine is to be connected to an external interface.
- The administrator of the machine should appropriately control the file of Job Log (Audit Log) data downloaded to, for example, a PC and ensure that none other than the administrator handles it.
- The administrator of the machine should check the Job Log (Audit Log) data at appropriate timing, thereby determining whether a security compromise or a faulty condition has occurred during an operating period.
- When generating or deleting Job Log (Audit Log) and Job Log (Audit Log) data, the administrator of the machine should check conditions of using this machine by the user.
- The administrator of the machine should make sure that each individual user updates the OS of the user's terminal and applications installed in it to eliminate any vulnerabilities.
- This machine allows the print function and the file box saving function to be used from the USB memory. The administrator of the machine should make sure that each individual user does not leave the machine with the USB memory inserted in it.

The administrator of the machine disables the following functions and operates and manages the machine under a condition in which those functions are disabled.

Function Name	Setting Procedure
IP Address Fax Function *	Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [Network Fax Settings] ▸▸ [Network Fax Function Settings], set [IP Address Fax Function] to [OFF].
Internet Fax Function *	Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [Network Fax Settings] ▸▸ [Network Fax Function Settings], set [Internet Fax Function] to [OFF].
Relay User Box	Using [Administrator Settings] ▸▸ [Fax Settings] ▸▸ [Function Settings] ▸▸ [Function ON/OFF Settings], set [Relay RX] to [OFF].
File Re-TX Box	Using [Administrator Settings] ▸▸ [Fax Settings] ▸▸ [Function Settings], set [Incomplete TX Hold] to [No].
PC-Fax Permission	Using [Administrator Settings] ▸▸ [Fax Settings] ▸▸ [Function Settings], set [PC-Fax Permission Setting] to [Restrict].
Bulletin Board User Box	• Do not create [Bulletin Board User Box] using [Utility] ▸▸ [One-Touch/User Box Registration] ▸▸ [Create User Box]. • Do not create [Bulletin Board User Box] using [Administrator Settings] ▸▸ [One-Touch/User Box Registration] ▸▸ [Create User Box].
Polling TX	Do not use [Polling TX] using [Menu] ▸▸ [Scan/Fax] ▸▸ [Application].
Delete Other User Jobs	Using [Administrator Settings] ▸▸ [System Settings] ▸▸ [Restrict User Access] ▸▸ [Restrict Access to Job Settings], set [Delete Other User Jobs] to [Restrict].
RAW Port Number	Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [TCP/IP Settings] ▸▸ [RAW Port Number], set [Port 1 to Port 6] to [OFF].
NetWare Settings	• Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [NetWare Settings], set [IPX Settings] to [OFF]. • Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [NetWare Settings], set [NetWare Print Settings] to [OFF].
FTP TX Settings	Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [FTP Settings], set [FTP TX Settings] to [OFF].
SMB Settings	• Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [SMB Settings], set [Client Settings] to [OFF]. • Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [SMB Settings], set [SMB Server Settings] to [OFF]. • Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [SMB Settings], set [WINS/NetBIOS Settings] to [OFF].
E-Mail RX (POP)	Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [E-Mail Settings], set [E-Mail RX (POP)] to [OFF].
SNMP Settings	Using [Administrator Settings] ▸▸ [Network Settings], set [SNMP Settings] to [OFF].
TCP Socket Settings	• Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [Forward (2/3)] ▸▸ [TCP Socket Settings], set [TCP Socket] to [OFF]. • Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [Forward (2/3)] ▸▸ [TCP Socket Settings], set [TCP Socket (ASCII Mode)] to [OFF].
SSL/TLS Version Setting	Start the PageScope Web Connection and, using [Security] ▸▸ [PKI Settings] ▸▸ [SSL Setting] of the administrator mode, cancel the selection of [SSLv3] of [SSL/TLS Version Setting].
Flash Display Setting	Start the PageScope Web Connection and, using [System Settings] ▸▸ [Flash Display Setting] of the administrator mode, set [Flash Display] to [Restrict].
WebDAV Settings	• Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [WebDAV Settings], set [WebDAV Client Settings] to [OFF]. • Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [WebDAV Settings], set [WebDAV Server Settings] to [OFF].

Function Name	Setting Procedure
DPWS Settings (Printer Settings/Scanner Settings)	• Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [DPWS Settings], set [Printer Settings] to [OFF]. • Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [DPWS Settings], set [Scanner Settings] to [OFF].
LPD Setting	Using [Administrator Settings] ▸▸ [Network Settings] ▸▸ [Detail Settings], set [LPD Setting] to [Disable].
Bluetooth Setting *	Using [Administrator Settings] ▸▸ [Network Settings], set [Bluetooth Setting] to [Invalid].
Manual destination entry prohibition	The administrator of the machine registers only fax destinations and E-mail addresses with S/MIME certificates.
External Memory Function Settings (Save Document)	Using [Administrator Settings] ▸▸ [System Settings] ▸▸ [User Box Settings] ▸▸ [External Memory Function Settings], set [Save Document] to [OFF].

*: It will not be displayed in case of service mode where the setting is not configured.

Machine Maintenance Control

The administrator of the machine should perform the following maintenance control activities.

- Provide adequate control over the machine to ensure that only the Service Engineer is able to perform physical service operations on the machine.
- Provide adequate control over the machine to ensure that any physical service operations performed on the machine by the Service Engineer are overseen by the administrator of the machine.
- Some options require that Enhanced Security Mode be turned [OFF] before they can be used on the machine. If you are not sure whether a particular option to be additionally purchased is fully operational with the Enhanced Security Mode turned [ON], contact your Service Representative.
- Install the machine at a safe site that can be monitored and operate and manage the machine while ensuring that the machine is protected from unauthorized physical access.

1.4 Miscellaneous

Password Rules

Study the following table for details of the number and types of characters that can be used for each password. For details of the settings of the Password Rules, see page 2-11.

Types of passwords	Number of characters	Types of characters	Conditions for setting/changes
Administrator Password	8 to 64 characters*	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, + • Special characters (68 characters) Selectable from among a total of 161 characters	• A password only consisting of identical characters cannot be registered or changed. • The current password must be entered before a change can be made in the setting. • A new password to be set should not be the same as the current one.
User Password			
Account Password			
Public User Box Password			
WebDAV Server Password			
Annotation User Box Password			
Secure Print Password	8 to 64 characters*	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, + Selectable from among a total of 93 characters	• A password only consisting of identical characters cannot be registered.
SNMP Password • auth-password • priv-password	8 to 32 characters*	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, $, %, &, (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [,], ^, _, `, {, |, }, ~, + Selectable from among a total of 90 characters	• A password only consisting of identical characters cannot be registered or changed. • The current password must be entered before a change can be made in the setting. • A new password to be set should not be the same as the current one.
Encryption Key	20 characters	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', *, +, -, ., /, =, ?, @, ^, _, `, {, |, }, ~ Selectable from among a total of 83 characters	• An Encryption Key only consisting of identical characters cannot be registered or changed. • The current Encryption Key must be entered before a change can be made in the setting. • A new Encryption Key to be set should not be the same as the current one.
Confidential RX password	8 characters	• Numeric characters: 0 to 9 • Symbols: *, #	• A password only consisting of identical characters cannot be registered or changed.
Memory RX User Box Password	1 to 8 characters	• Numeric characters: 0 to 9	• The password rules are not applicable.
Encrypted PDF Password	-	-	• The password rules are not applicable. • Password that is set when PDF document is created.

*: The minimum number of characters set in [Set Minimum Password Length] must be set for the password. The default value is 12.

Precautions for Use of Umlaut

- Setting or entering an umlaut from the control panel may be disabled depending on the setting made in this machine, but not on the client PC side including PageScope Web Connection. If an umlaut is set in a password on the PC side, therefore, the umlaut cannot be entered from the control panel, which means that this particular password is not usable.

Precautions for Use of Various Types of Applications

Comply with the following requirements when using the PageScope Web Connection or an application of various other types.
The administrator of the machine should make sure that the user observes the following requirements.

- The password control function of each application stores the password that has been entered in the PC being used. Disable the password management function of each application and perform an operation without storing a password.
  Use a web browser or an application of various other types that shows "*" or "●" for the password entered.
- Once the password has been entered, do not leave your PC idle without logging on.
- Set the web browser so that cache files are not saved.
- Do not access any other site once you have logged onto the machine with the PageScope Web Connection. Accessing any other site or a link included in e-mail, in particular, can lead to execution of an unintended type of operation. Whenever access to any other site is necessary, be sure first to log off from the machine through the PageScope Web Connection.
- Using the same password a number of times increases the risk of spoofing.
- If a web browser such as Internet Explorer is used on the client PC side, "TLS v1" should be used for the SSL setting.
- Expanded functions, which can be used in association with applications by registering the optional License Kit, are available, including collecting and controlling user and account information by means of the WebDAV function. Use of these expanded functions is not covered by certification of ISO15408.
- Optional applications not described in this User's Guide are not covered by certification of ISO15408.

Encrypting communications

The following are the cryptographic algorithms of key exchange and communications encryption systems supported in generation of encryption keys.

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

NOTICE

The administrator of the machine should make sure that SSL encryption communication is not performed with the SSL set in SSL v3.

Do not use an SSL certificate that is electronically signed by MD5, as an increased risk results of data to be protected being tampered with or leaked.

To eliminate the risk of the data to be protected being tampered with or leaked, refer to the recommended ciphers list disclosed by, for example, NIST and CRYPTREC and use the appropriate cryptographic technique.

Use the following browsers to ensure SSL encryption communication with appropriate strength. Use of any of the following browsers achieves SSL encryption communication that ensures confidentiality of the image data transmitted and received.

Microsoft Internet Explorer

- 6/7/8/9/10 (desktop version)

Mozilla Firefox

- 3.5 or later
- ESR 10.0 or later

Microsoft Internet Explorer 8 is used for the ISO15408 evaluation for this machine.

Print functions

Only the following procedures are guaranteed for the print functions performed from the client PC.

- Use IPPS printing for the print functions performed using the printer driver.
- Use direct printing from the PageScope Web Connection for the print functions not performed via the printer driver.

IPP printing

IPP (Internet Printing Protocol) is a function that allows Secure Print documents and image data stored in boxes to be printed via the Internet by using the HTTP (HyperText Transfer Protocol) of the TCP/IP Protocol. IPPS (IPP over SSL/TLS) is the type of IPP that performs the SSL encryption communication.

<Installing printer driver>

To perform IPP printing, the printer driver must be installed. From "Add Printer Wizard", type the IP address of this machine in the following format in the "URL" field.

To set IPP printing:

- Type "http://<IP address of the machine>/ipp"

To set IPPS printing:

<In Windows XP/Server 2003>

- Type "https://<IP address of the machine>/ipp"

<In Windows Vista/7/Server 2008/Server 2008 R2/Server 2012>

- Type "https://[host name].[domain name]/ipp"

For [Host Name] and [Domain Name], specify the names set with the DNS server.

<Registering the certificate in Windows Vista or later>

Windows Vista or later, which offers enhanced security functions, gives a certificate error message if the SSL certificate is one that is not issued by a certification body. In such cases, it becomes necessary to register the certificate of this machine as that issued by a reliable party for the computer account.

First, register Host Name and IP address of this machine in the DNS server in advance. Then, in TCP/IP Settings of PageScope Web Connection, set the DNS Host Name and DNS Default Domain Name registered with the DNS server.

It should also be noted that, for the certificate to be imported, a certificate for SSL encryption communication should be registered in PageScope Web Connection and exported in advance as the certificate including the public key.

1 From "Continue to this website," call the PageScope Web Connection window to the screen.

2 Click "Certificate Error" to display the certificate. Then, click "Install Certificate" to install the certificate.

3 Display the physical stores. Then, deploy the certificate, which has earlier been exported, in "Local Computer" of "Trusted Root Certification Authorities" to thereby import the certificate.

Items of Data Cleared by Overwrite All Data Function

The Overwrite All Data function clears the following items of data.

Items of Data Cleared	Description
Password Rules	Sets [Invalid] and disables [Set Minimum Password Length]
User registration data	Deletes all user-related data that has been registered
Account track registration data	Deletes all account track-related data that has been registered
Box registration data/file	Deletes all User Box-related information and files saved in User Box
Secure Print ID/Password/ document	Deletes all Secure Print document-related information and files saved
ID & Print document	Deletes all ID & Print documents saved in ID & Print User Box
Image files	• Image files other than Secure Print documents, ID & Print documents, and User Box files • Data files left in the HDD data space, used as image files and not deleted through the general deletion operation • Temporary data files generated during print image file processing
Destination recipient data files	Deletes all destination recipient data including e-mail addresses and telephone numbers
Encryption Key	Clears the currently set Encryption Key
Administrator Password	Clears the currently set password, resetting it to the factory setting (1234567812345678)
SNMP Password	Clears the currently set password, resetting it to the factory setting (MAC address)
WebDAV Server Password	Clears the currently set password, resetting it to the factory setting (sysadm)
S/MIME certificate	Deletes the currently set S/MIME certificate
Device certificate (SSL certificate)	Deletes the currently set Device certificate (SSL certificate)
SSL encryption strength	Deletes the SSL certificate to thereby clear the SSL encryption strength
SSL-compliant protocol	Makes the protocol not complying with SSL
Network Setting	Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, and AppleTalk Printer Name setting), resetting it to the factory setting
Daylight Saving Time	Set to [No]
Time Adjustment Setting (NTP)	Set to [OFF]
Time/date data	Varies corrected data, if the time-of-day data is corrected due to, for example, the daylight saving time

Fax functions

An optional Fax Kit is required for using fax functions. Contact your Service Representative.

USB keyboard

The USB keyboard is not used for the ISO15408 evaluation for this machine.

Do not use the USB keyboard.

Different types of boxes

A box may be a user box or a system box. The user can store documents in the User Box. Also, the user can print a file from the User Box or send a file to another user. The System Box is used by the system to temporarily store files when the user uses the facsimile or print function together with the file storage function of the box.

Type	Description
Public User Box	This is the public box in which all users can store documents and use them. Note that a password is set for the box and the set password needs to be entered before access can be gained to the box.
Personal User Box	This is a personal box. Only users who have logged in to the system can store and use documents in the Personal User Box.
Group User Box	This is a group box. Only users belonging to the same department (or group) can store and use documents in the Group User Box.
Secure Print Box	When you print a document from the PC or when you select the Secure Print function using the printer driver, this data file is stored in the Secure Print User Box.
Memory RX Box	When a facsimile is received by the Memory RX function, it is stored in the Memory RX User Box.
ID & Print Box	When you print a document from the PC, the files transferred with the ID & Print function are stored in the ID & Print User Box.
Annotation User Box	When a stored file is printed out or sent to another user, its date, time and any annotations are added to this box automatically.
Password Encrypted PDF Box	When a password protected PDF file is printed out or stored in the User Box, the file is stored in the Password Encrypted PDF User Box.

Hardware and software used in the machine

The following lists the types of hardware and software and their versions used for the ISO15408 evaluation for this machine.

The user should appropriately manage the hardware and software used with the machine on his or her own responsibility.

Hardware/software	Version, etc.
FAX Kit	FK-511
Printer Driver	KONICA MINOLTA 754 Series • PCL Ver. 3.1.0.0 or later • PS Ver. 3.1.0.0 or later • XPS Ver. 3.1.0.0 or later
PageScope Data Administrator	Ver. 4.1.24000.05011 or later
External authentication server	Active directory mounted on Windows Server 2008 R2 Standard Service Pack 1
DNS server	Windows Server 2003 R2 Standard Edition Service Pack 2

Firmware integrity verification function

When the main power switch is turned ON with the Enhanced Security Mode set to [ON], the machine checks the encryption key and the hash value to thereby determine that its firmware is fully operational.

If a fault occurs in the firmware, a malfunction screen appears when the machine is started, warning that a fault has occurred. To reset the fault condition, turn [OFF] the Enhanced Security Mode and restart the machine, or update the firmware. For more details, consult your Service Representative.

IPsec setting

This machine offers a choice of two authentication methods of [Pre-Shared Key] and [Digital Signature] for authenticating the remote machine with which to communicate.

When [Pre-Shared Key] is to be used, control the pre-shared key appropriately to ensure that it is not leaked to any third party other than the remote machine with which to communicate.

[Digital Signature] has a higher security strength than [Pre-Shared Key].

CS Remote Care function

CS Remote Care is a system that manages the machine through transmission and reception of various types of data for managing the machine between the machine and the CS Remote Care center computer via a telephone/fax line, a network, or E-mail.

When the Enhanced Security Mode is set to [ON], the following functions are no longer usable: instructing to rewrite the firmware, sending and receiving account counter information, rewriting settings of the machine, and the Counter Remote Control function.

Terminating a Session and Logging out

The machine allows the operator to automatically log out from or terminate a session, if it is unable to detect an operation on the control panel or a communication packet on the network.

The following shows the setting range and the default setting of each function. Set the time according to the environment in which the machine is used.

The administrator of the machine should explain to the user that the following settings are made. The administrator of the machine should also explain to the user immediately as soon as the setting has been changed.

Function name/software, etc	Description
System Auto Reset	Setting range • [1] to [9] minutes, Default setting: [1] minute Setting procedure • [Utility] ▸▸ [Administrator Settings] ▸▸ [System Settings] ▸▸ [Reset Settings] ▸▸ [System Auto Reset]
Auto Logout (PageScope Web Connection)	Setting range • [Admin. Mode Logout Time]: [1] to [60] minutes Default setting: [10] minutes • [User Mode Logout Time]: [1] to [60] minutes Default setting: [60] minutes Setting procedure • Start the PageScope Web Connection and, in the Administrator Mode, select [Security] ▸▸ [Auto Logout].
PageScope Data Administrator	Default setting: [60] minutes (No change can be made in the setting) The time setting represents consideration for the time-consuming task, such as downloading the registered information. Be careful about leaving your seat, because the time setting is rather long.

Authentication error during external server authentication

If a user is unable to log in successfully during user authentication using the external server authentication, possible causes include the status of connection to the external server, the condition of the external server (the server is down), and the status of user registration with the external server such as the number of users to be controlled by the machine reaching its limit and the user password quality on the external server.

The administrator of the machine should check these points and make the appropriate settings.

2 Administrator Operations

2 Administrator Operations

2.1 Accessing the Administrator Settings

In Administrator Settings, the settings for the machine system and network can be registered or changed.

This machine implements authentication of the user of the Administrator Settings function through the Administrator Password that verifies the identity as the administrator of the person who accesses the function. During the authentication procedure, the Administrator Password entered for the authentication purpose appears as "*" or "●" on the display.

When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

NOTICE

Make sure that none of the general users of the machine will know the Administrator Password.

If the Administrator Password is forgotten, it must be set again by the Service Engineer. Contact your Service Representative.

2.1.1 Accessing the Administrator Settings

The machine does not accept access to the Administrator Settings under any of the following conditions. Wait for some while before attempting to gain access to the Administrator Settings again.

- The Administrator Settings has been logged on to through access made from the PC.
- A remote operation is being performed from an application on the PC.
- There is a job being executed by the machine.
- There is a reserved job (timer TX, fax redial waiting, etc.) in the machine.
- Immediately after the main power switch has been turned ON.
- A malfunction code is displayed on the machine.

<From the Control Panel>

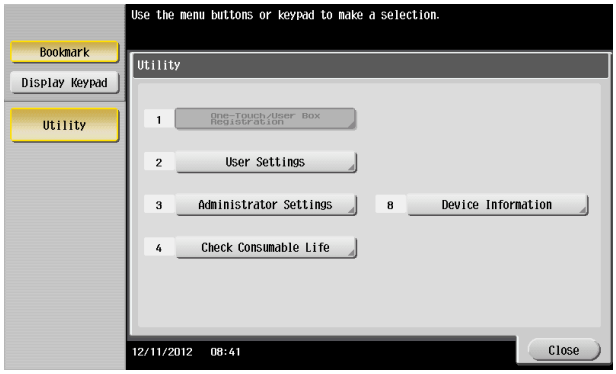
✔ When accessing the Administrator Settings from the control panel, if you have already logged on to the Administrator Settings using PageScope Web Connection, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Administrator Settings once again.

✔ When accessing the Administrator Settings from the control panel, if [Export to the device] operation is being executed using the PageScope Data Administrator, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Administrator Settings once again.

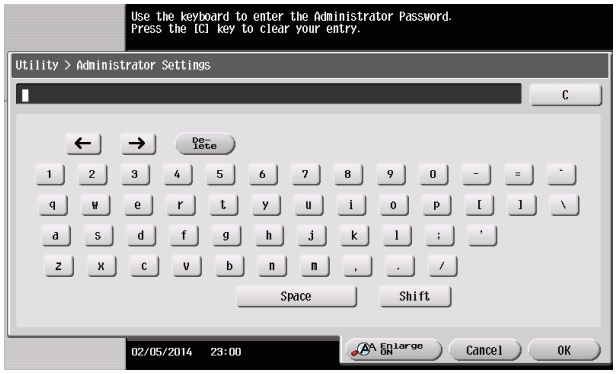
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Touch [Menu] ▸▸ [Utility].

2 Touch [Administrator Settings].



3 Enter the Administrator Password from the keyboard.



➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

4 Touch [OK].

➔ If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.
➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

5 Press the [Reset] key to log off from the Administrator Settings.

2.1.2 Accessing the User Mode

You can log on to the User Mode as an administrator. In the User Mode, you can check or delete a job, which is disabled in Administrator Settings.

Reference

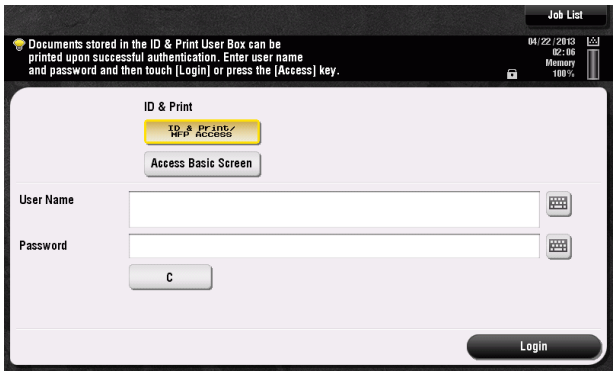
- The authority relating to box settings is the same as that of Administrator Settings.

<From the Control Panel>

✔ The administrator must first make User Authentication settings before he or she can access User Mode. For details of the User Authentication, see page 2-20.

✔ Do not leave the machine with the User Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the User Mode.

1 Touch the keyboard icon in the [User Name] field.



2 Enter "admin" in [User Name]. Enter the password set for this machine in [Password].

➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the previous screen.

3 Touch [OK].

4 Touch [Access] or [Login].

➔ If a wrong Administrator Password is entered, a message that tells that the authentication has failed appears. Enter the correct Administrator Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

5 Touch [Access] or [Close] to log off from the User Mode.

<From PageScope Web Connection>

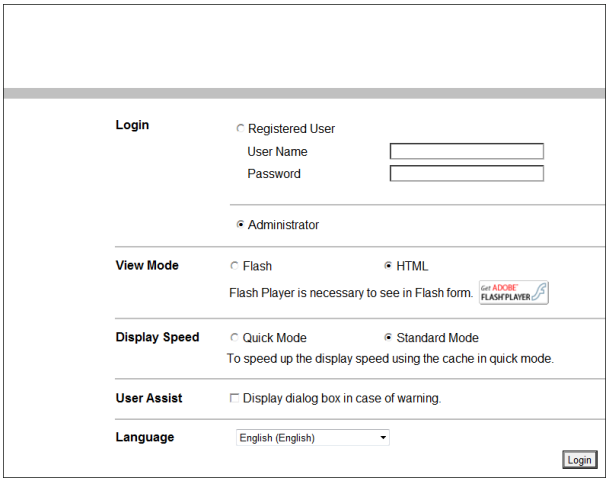
- ✔ While you are logging onto the Admin Mode using PageScope Web Connection, any operations from the machine's control panel are disabled.
- ✔ If you have already logged on to the Admin Mode from the control panel or using PageScope Web Connection, the machine displays a message that tells that another administrator has previously logged on and rejects any attempt to log on to the Admin Mode using the PageScope Web Connection. Click [OK] and wait for some while before attempting to access the Admin Mode once again.
- ✔ If [Export to the device] operation is being executed using the PageScope Data Administrator, the machine displays a message that tells you cannot log on to the mode because of the remote operation being performed and rejects any attempts to the Admin Mode via the PageScope Web Connection. Click [OK] and wait for some while before attempting to access the Admin Mode once again.
- ✔ If an attempt is made to log on to the Admin Mode while a job is being executed, the machine gives a message that tells that it is now impossible to log on to the Admin Mode. Click [OK] and try logging on to the Admin Mode after the execution of the job is completed.
- ✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- ✔ If you have logged on to the Admin Mode using the PageScope Web Connection and if you close the web browser without clicking [Logout], the control panel remains locked for 70 sec.
- ✔ Different initial screens appear after you have logged on to the Admin Mode depending on the Customize setting. The descriptions herein given are concerned with the display screen set in [Meter Counter] of Maintenance.

1 Start the Web browser.

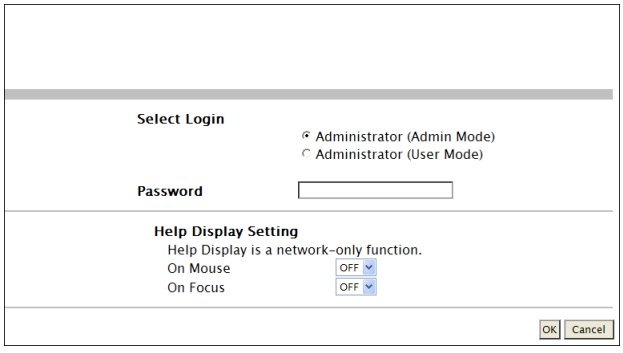
2 Enter the IP address of the machine in the address bar.

3 Press the [Enter] key to start PageScope Web Connection.

4 Click the Administrator radio button and [Login].



5 Select "Administrator (Admin Mode)" or "Administrator (User Mode)" and enter the Administrator Password in the "Password" box.



➔ If "Administrator (Admin Mode)" is selected, the settings for the machine system and network can be registered or changed.

➔ If "Administrator (User Mode)" is selected, you can log on to the User Mode as an Administrator. In the User Mode, you can check or delete a job, which is disabled in Administrator Settings. Note, however, that the authority relating to box settings is the same as that of Administrator Settings.

➔ When accessing the Admin Mode using the PageScope Web Connection, enter the same Administrator Password as that for the machine.

6 Click [OK].

➔ If a wrong Administrator Password is entered, a message that tells that the authentication has failed appears. Enter the correct Administrator Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

7 Click [Logout].

8 Click [OK].

This allows you to log off from the Admin Mode.

2.2 Enhancing the Security Function

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the Enhanced Security Mode that allows settings for enhancing each of different security functions to be converted all at once.

In the Enhanced Security Mode, the machine allows selection of whether to use the Enhanced Security Mode or not. If the Enhanced Security Mode is set to [ON], a count is taken of the number of unauthorized accesses to the Administrator Settings, User Authentication, Account Track, SNMP authentication, WebDAV authentication, all Secure Print, and all User Boxes. A function is also set that determines whether each password meets predetermined requirements. The security function is thus enhanced in the Enhanced Security Mode.

The following settings must first be made before the Enhanced Security Mode is set to [ON].

NOTICE

First, set the Encryption Key. To set the Encryption Key, HDD Format must first be executed. Execution of the HDD Format clears various setting values. For details of items that are cleared by HDD Format, see page 2-10.

If initialization is executed by the Service Engineer, the Password Rules are set to [Invalid] and the Administrator Password is reset to the factory setting (1234567812345678). To set the Administrator Password and turn [ON] the Enhanced Security Mode again.

Settings to be Made in Advance	Description
Administrator Password	Meet the Password Rules. The factory setting is "1234567812345678."
User Authentication	Check that [Authenticate] (the server type is Active Directory only for External Server Authentication) is set.
Encryption Key	Set the Encryption Key.
Certificate for SSL	Register the self-signed certificate for SSL communications.
Service settings	Calls for setting made by the Service Engineer. For details, contact your Service Representative.

Setting the Enhanced Security Mode to [ON] changes the setting values of the following functions.

NOTICE

If an attempt is made to change a setting that has been changed as a result of setting the Enhanced Security Mode to [ON], a screen may appear indicating that the Enhanced Security Mode is to be canceled. Note that executing this screen will cancel the Enhanced Security Mode.

The description "not to be changed" given in parentheses in the table below indicates that the specific setting cannot be changed with the Enhanced Security Mode set to [ON].

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
Password Rules	Invalid	Enable (not to be changed) * If [Enable] is set for Password Rules, the types and number of characters to be used for each password are limited. For details of the Password Rules, see page 1-11.
Prohibited Functions When Authentication Error	Mode 1	Mode 2 (not to be changed): Three times is set. * The number of times can be changed to once, twice, or three times (twice, four times, or six times for the WebDAV Server Password).
Release Time settings	5 min.	The setting value should be 5 min. or more (no value less than 5 can be set)
Confidential Document Access Method	Mode 1	Mode 2 (not to be changed) * In association with Prohibit Functions When Authentication Error, the method is changed from authentication using Secure Print ID and password (Mode 1) to that using the password with the Secure Print document first narrowed down by Secure Print ID (Mode 2).
Secure Print User Box Preview	Thumbnail View, Detail View, and Document Details are enabled	Only Detail View is enabled before password authentication (Mode 2)

Function Name	Factory Setting	When Enhanced Security Mode is set to [ON]
Public User Access	Restrict	Restrict (not to be changed)
User Name List	OFF	OFF (not to be changed)
Print Without Authentication	Restrict	Restrict (not to be changed)
User Box Administrator Setting	Restrict	Restrict (not to be changed)
Mode using SSL/TLS	None	Admin. Mode and User Mode (not to be changed)
SSL Encryption Strength	AES-256, 3DES-168, RC4-128, DES-56, RC4-40	AES/3DES (not to be changed to one containing strength lower than AES/3DES)
Automatically Obtain Certificates of S/MIME	No	No (not to be changed)
S/MIME Encryption Method	3DES	3DES (not to be changed to DES or RC-2)
FTP Server	ON	OFF (not to be changed)
SNMPv1/v2c Settings	Read setting: Enable Write setting: Enable	Read setting: Enable, Write setting: Invalid (not to be changed)
SNMP v3 Settings Security Level and auth-password/priv-password	auth-password/ priv-password	The security level can be selected from among [auth-password] and [auth-password/priv-password]. Auth-password and priv-password can both be set.
Print Data Capture	Allow	Restrict (not to be changed)
Network Setting Clear (Pagescope Web Connection)	Enabled	Restrict
Registering and Changing Address by the user (Address Book and Program)	Allow	Restrict (not to be changed)
Initialize (Network Settings)	Enabled	Restrict (not to be changed)
Image Log Transfer Settings	OFF	OFF (not to be changed)
CS Remote Care	Usable	Remote device setting disabled
Counter Remote Control	Restrict	Restrict (not to be changed)
Remote Panel Settings (Server Settings/Client Settings)	OFF	OFF (not to be changed)
Print Simple Auth. (Authentication Setting)	Restrict	Restrict (not to be changed)
External Application Connection	Yes	No (not to be changed)
E-mail RX Print	OFF	OFF (not to be changed)
Machine Update Settings	No	No (not to be changed)
IWS Settings	OFF	OFF (not to be changed)
HDD backup data Settings	Restrict	Restrict (not to be changed)

2.2.1 Items cleared by HDD Format

Following are the items that are cleared by HDD Format.

Whenever HDD Format is executed, be sure to set the Enhanced Security Mode to [ON] again.

Items of Data Cleared	Description
Enhanced Security Mode	Set to [OFF]
Device certificate (SSL certificate)	Deletes the device certificate (SSL certificate) registered in the machine
SSL encryption strength	Deletes the SSL certificate to thereby clear the SSL encryption strength
SSL-compliant protocol	Makes the protocol not complying with SSL
User Authentication	Set to [OFF]
Account Track Authentication	Set to [OFF]
User Box Administrator	Set to [Restrict]
Public User Access	Set to [Restrict]
User Name List	Set to [OFF]
Print Simple Auth.	Set to [Restrict]
Print Without Authentication	Set to [Restrict]
User registration data	Deletes all user-related data that has been registered
Account Track registration data	Deletes all account track-related data that has been registered
Box registration data/file	Deletes all User Box-related information and files saved in User Box
Secure Print ID/Password/document	Deletes all Secure Print document-related information and files saved
Destination recipient data files	Deletes all destination recipient data including e-mail addresses and telephone numbers
S/MIME certificate	Deletes the currently set S/MIME certificate

2.2.2 Setting the Password Rules

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

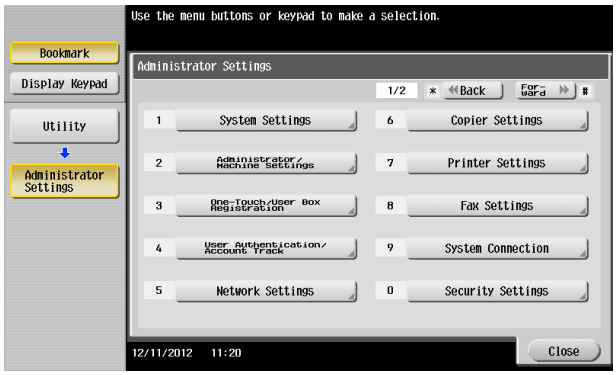
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

NOTICE

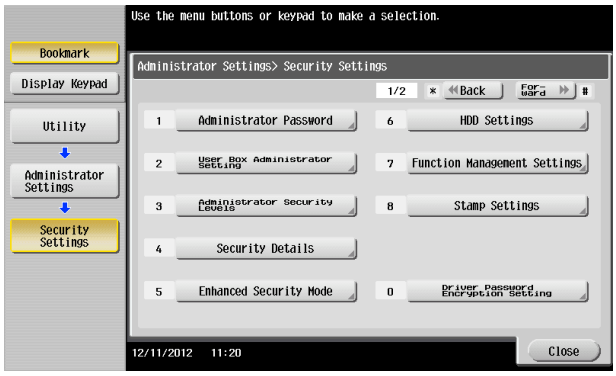
Before enabling the Password Rules, change the currently set password so as to meet the Password Rules. For details of the Password Rules, see page 1-11.

1 Call the Administrator Settings on the display from the control panel.

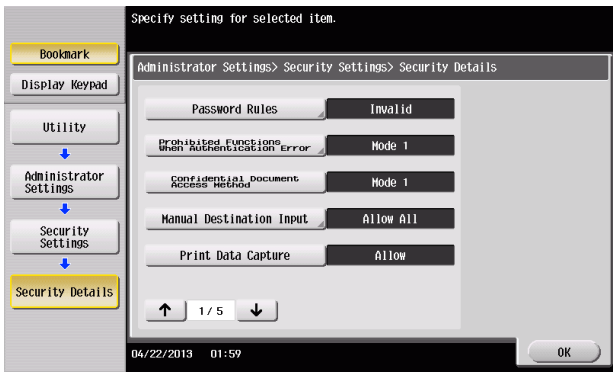
2 Touch [Security Settings].



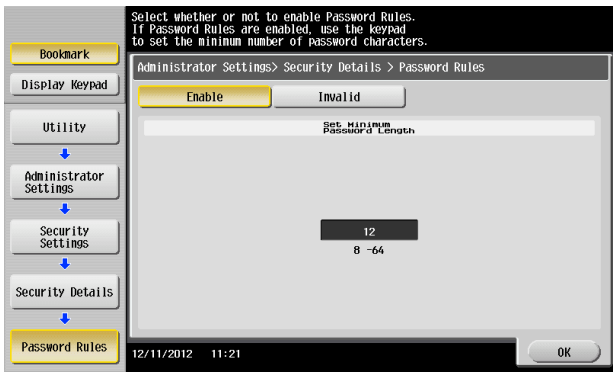
3 Touch [Security Details].



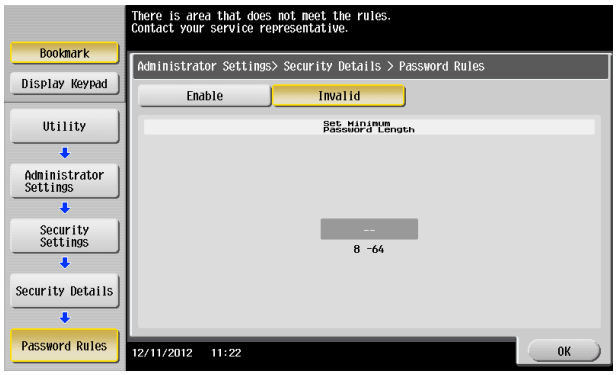
4 Touch [Password Rules].



5 Select [Enable] and set [Set Minimum Password Length] (8 to 64 characters).



➔ The following screen appears if the previously required settings are yet to be made by the Service Engineer. Contact your Service Representative.



6 Touch [OK].

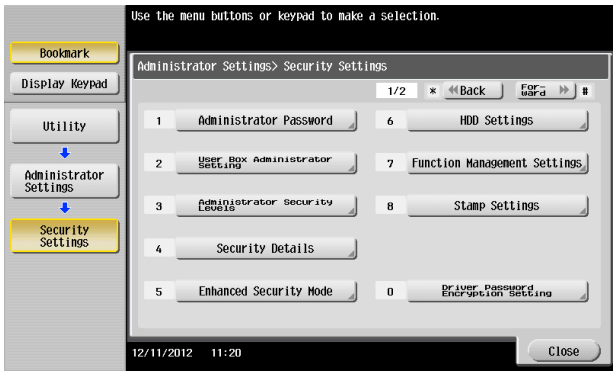
2.2.3 Setting the Enhanced Security Mode

- ✔ For the procedure to call the Administrator Settings on the display, see page 2-2.
- ✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✔ The Enhanced Security Mode is factory-set to [OFF]. Be sure to turn [ON] the Enhanced Security Mode so as to enable the security function of the machine.

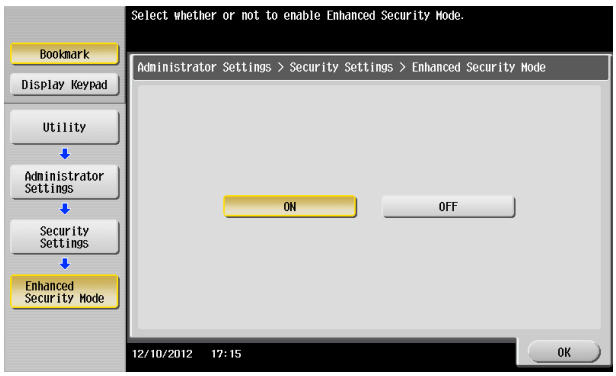
1 Call the Administrator Settings on the display from the control panel.

2 Touch [Security Settings].

3 Touch [Enhanced Security Mode].



4 Select [ON] to enable the Enhanced Security Mode and touch [OK].

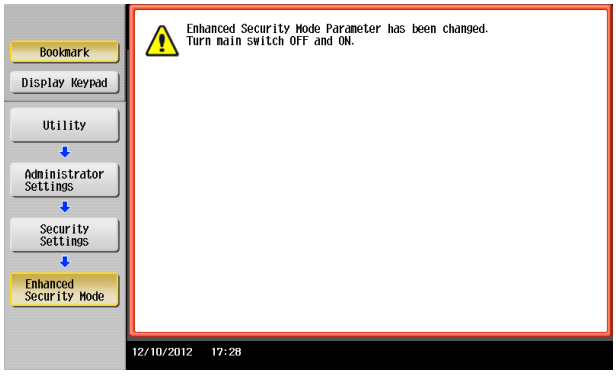


➔ The following screen appears if the previously required settings are yet to be made by the administrator of the machine. Make the necessary settings according to the corresponding set procedure.

➔ The following screen appears if the previously required settings are yet to be made by the Service Engineer. Contact your Service Representative.

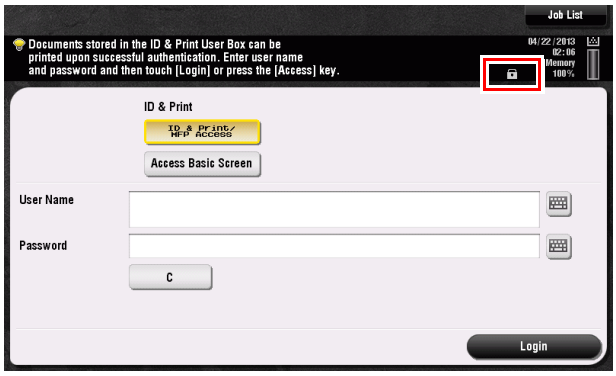
5 Any external applications registered using OpenAPI will be deleted when the Enhanced Security Mode is set to [ON]. A confirmation message appears. Select [Yes] and touch [OK].

6 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

➔ If the Enhanced Security Mode is properly set to [ON], a key icon appears at the portion on the screen enclosed by a red frame, indicating that the machine is in the Enhanced Security Mode.



2.3 Preventing Unauthorized Access

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of Prohibited Functions When Authentication Error. The machine then takes a count of the number of unsuccessful accesses to the Administrator Settings, User Authentication, Account Track, SNMP authentication, WebDAV authentication, Secure Print authentication, and User Box authentication to prohibit the authentication operation.

Either [Mode 1] or [Mode 2] can be selected for Prohibited Functions When Authentication Error. The factory setting is [Mode 1]. If the Enhanced Security Mode is set to [ON], the setting is changed to [Mode 2] (check count: three times). It is nonetheless possible to change the check count to select from among once, twice, or three times (twice, four times, or six times for the WebDAV authentication).
If [Mode 2] is selected, the Release Time Settings function is enabled. When the Administrator Settings is set into the access lock state, the main power switch is turned off and on and, after the lapse of a predetermined period of time after the machine is turned on again, the access lock state of the Administrator Settings is canceled. The Release Time Settings function allows the period of time, after the lapse of which the access lock state of the Administrator Settings is canceled, to be set in the range between 1 and 60 min. The factory setting is 5 min. For details of each mode, see the table below.

Mode	Description
Mode 1	If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec.
Mode 2	If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec. The number of times, in which authentication fails, is also counted and, when the failure count reaches a predetermined value, the authentication operation is prohibited and the machine is set into an access lock state.

NOTICE
If the access lock state of the Administrator Settings is canceled by the Service Engineer, the setting of the Release Time Settings function is not applied.

Making any of the following settings when the Enhanced Security Mode is set to [ON] will cancel the Enhanced Security Mode.

- Changing [Prohibited Functions When Authentication Error] to [Mode 1]
- Changing the check count for [Prohibited Functions When Authentication Error] to four times or more
- Setting [Release Time Settings] to 1 to 4 min.

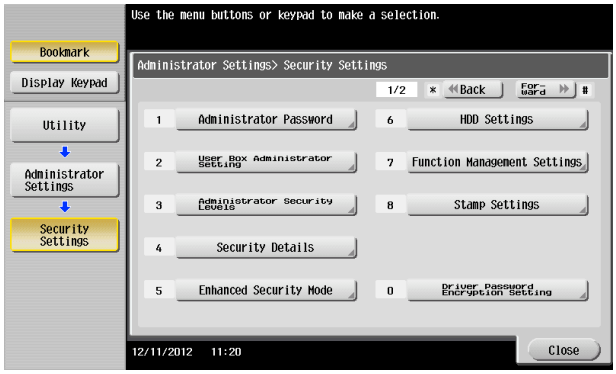
Setting Prohibited Functions When Authentication Error

✔ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-13.

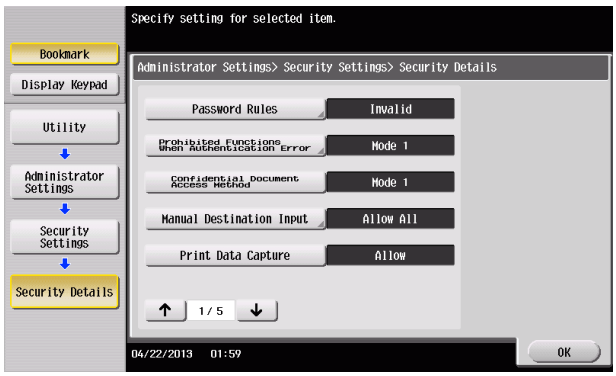
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Security Settings screen on the display from the control panel.

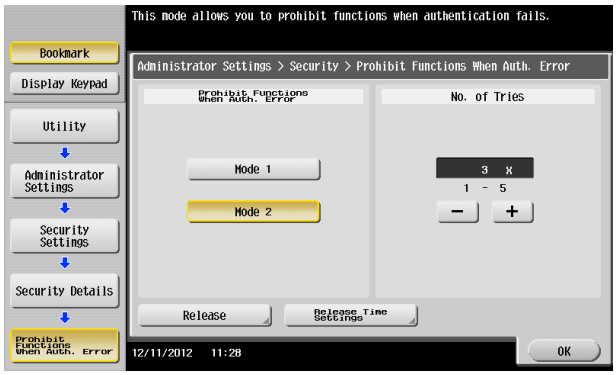
2 Touch [Security Details].



3 Touch [Prohibited Functions When Authentication Error].



4 Touch [Mode 2].



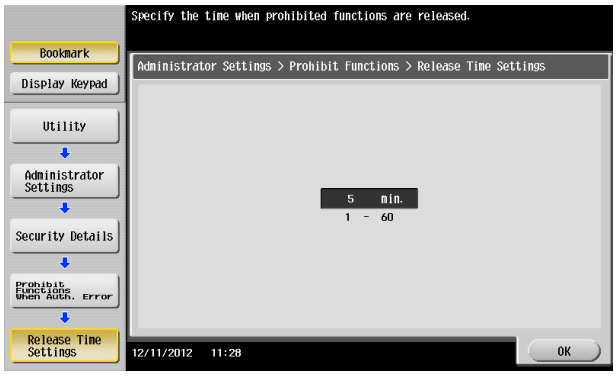
➔ Select [Mode 2] when the Enhanced Security Mode is set to [ON]. Selecting [Mode 1] will cancel the Enhanced Security Mode.

➔ Set three times or less when the Enhanced Security Mode is set to [ON]. Setting four times or more will cancel the Enhanced Security Mode.

➔ To change the check count, touch [+] to increase the count or [-] to decrease it.

5 Touch [Release Time Settings].

6 Touch [C] and, from the keypad, enter the time, after the lapse of which the access lock state of the Administrator Settings is canceled.



➔ Touch [Display Keypad] to display the keypad.

➔ Release Time can be set to any value between 1 min. and 60 min. in 1-min. increments. An input data error message appears when any value falling outside the range of 1 to 60 min. is set. Enter the correct Release Time.

➔ Set 5 min. or more when the Enhanced Security Mode is set to [ON]. Setting 1 to 4 min. will cancel the Enhanced Security Mode.

7 Touch [OK].

2.4 Canceling the Operation Prohibited State

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables the operation of Release Setting performed for canceling the state of Prohibited Functions When Authentication Error (access lock state) as a result of unauthorized access.

Release Setting clears the unauthorized access check count for all User Authentication, Account Track, SNMP authentication, WebDAV authentication, all Secure Print authentication, and all User Box authentication, resetting it to zero and canceling the operation prohibited state. Perform the following procedure to cancel the operation prohibited state.

Operation Prohibited State	Canceling procedure
Administrator Settings	• The Service Engineer touches [Administrator unlocking] to cancel the operation prohibited state. • The operation prohibited state is canceled after the main power switch is turned off and on and the period of time set in [Release Time Settings] elapses.
User/Account authentication	The Administrator touches [Release] to cancel the operation prohibited state.
Secure Print authentication	
User Box authentication	
SNMP authentication	
WebDAV authentication	

Performing Release Setting

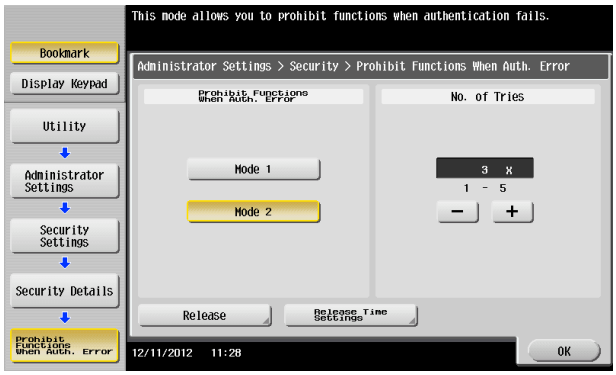
✔ For the procedure to call the Prohibited Functions When Authentication Error screen on the display, see steps 1 through 3 of page 2-16.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

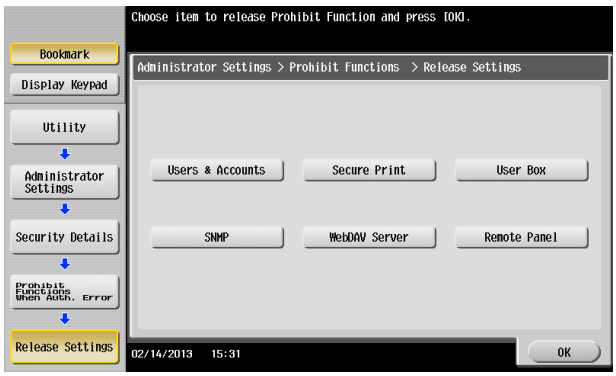
✔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

1 Call the Prohibited Functions When Authentication Error screen on the display from the control panel.

2 Touch [Release].



3 Select the function, for which Prohibit Function as a result of unauthorized access is to be released.



➔ The Remote Panel function cannot be used when the Enhanced Security Mode is set to [ON].

4 Touch [OK].

This clears the unauthorized access check count of the specific function selected in step 4 and cancels the operation prohibited state.

2.5 Setting the Authentication Method

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the authentication method for User Authentication and for Account Track.

The following three types of authentication methods available for User Authentication.

Mode	Description
[ON (MFP)]	The authentication function of this machine is used for user authentication.
[External Server Authentication]	Interacts with the authentication server used for user authentication in the operating environment.
[Main + External Server]	The authentication function of the machine may also be used, in consideration of a possible problem occurring in the external authentication server.

The Account Track authentication method may be set to [ON] or [OFF]. If [ON] is selected, be sure to set [Synchronize] in [Synchronize User Authentication & Account Track].

NOTICE

Changing the Account Track setting erases all user and account information data that has previously been registered. At this time, Personal User Boxes owned by the users who are deleted and Group User Boxes owned by the accounts that are deleted may be deleted or changed to Public User Boxes.
If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

If [External Server Authentication] is selected for the authentication method, be sure to select [Active Directory] in the External Server Settings.

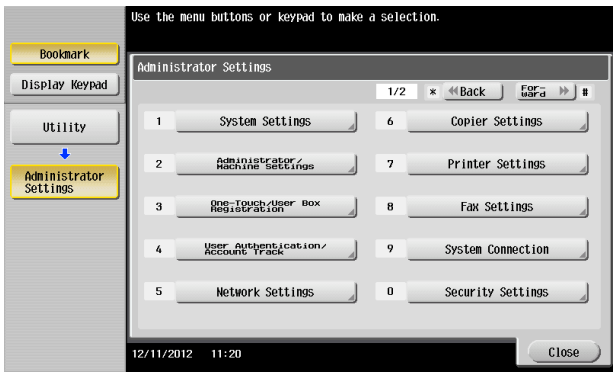
2.5.1 Setting the Authentication Method

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

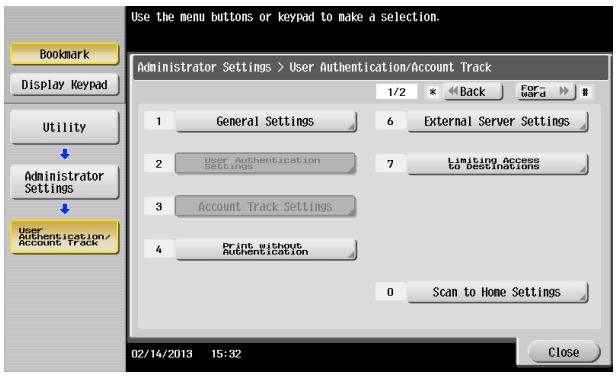
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Administrator Settings on the display from the control panel.

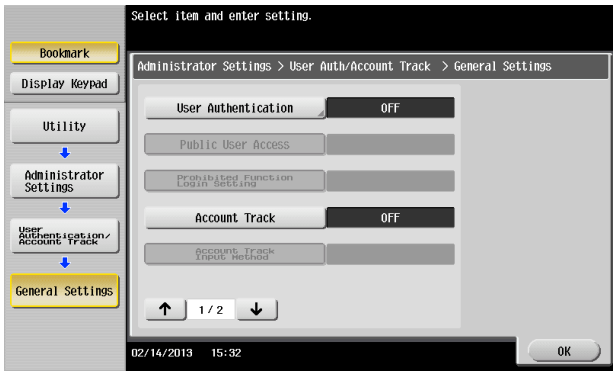
2 Touch [User Authentication/Account Track].



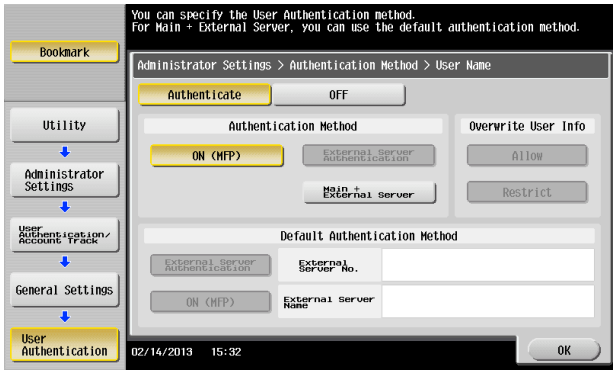
3 Touch [General Settings].



4 Touch [User Authentication].



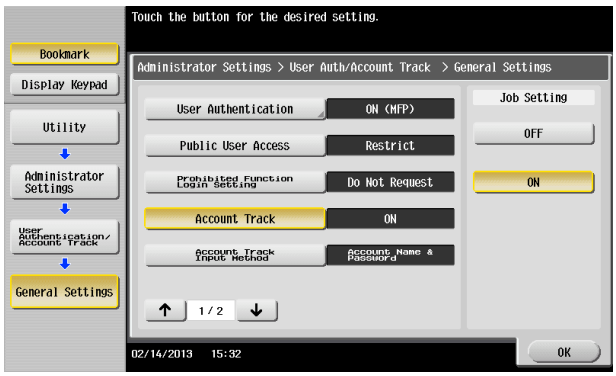
5 Select [Authenticate] and then select the authentication method.



➔ To use the External Server, the External Server must be registered in advance. For how to make the External Server Settings, see page 2-23.

6 Touch [OK].

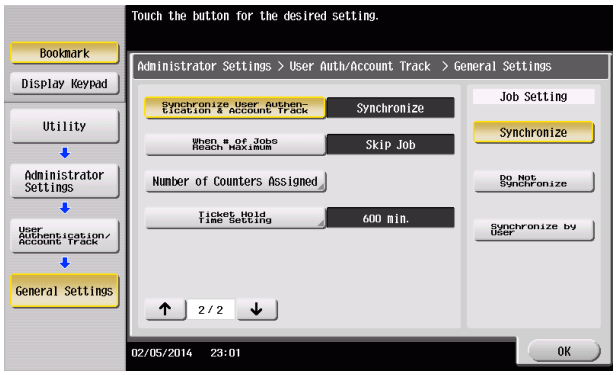
7 Select [Account Track] and touch [ON].



➔ If the Account Track is not to be used, go to step 10.

8 Touch [↓].

9 Select [Synchronize User Authentication & Account Track] and touch [Synchronize].



➔ When [Do Not Synchronize] is selected, both User Authentication and Account Track are checked each time the machine is used.

➔ If [Synchronize by User] is selected, [User Settings] shows [Synchronize User Auth. and Account Track], allowing the user to set whether to synchronize.

10 Touch [OK].

11 A message appears that prompts you to clear the use control data. Now, select [Yes] and touch [OK].

2.5.2 Setting the External Server

- ✔ If [External Server Authentication] is selected for the authentication method, the External Server must be registered in the machine in advance.
- ✔ For the procedure to call the User Authentication/Account Track screen on the display, see steps 1 and 2 of page 2-20.
- ✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

NOTICE

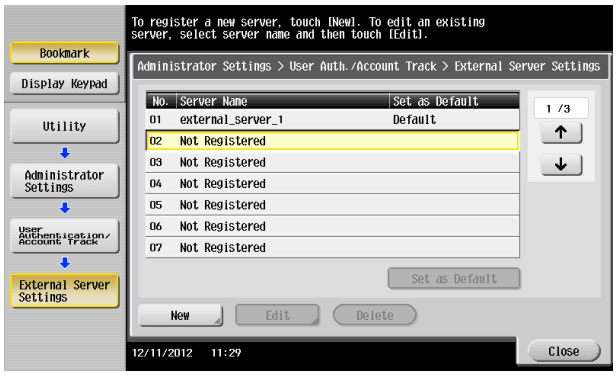
Set 3DES or higher for the encryption level and SHA-1 or higher for the hashing function with the Kerberos protocol of the Active Directory.

1 Call the User Authentication/Account Track screen on the display from the control panel.

2 Touch [External Sever Settings].

3 Touch the specific Sever Registration key, in which no sever has been registered.

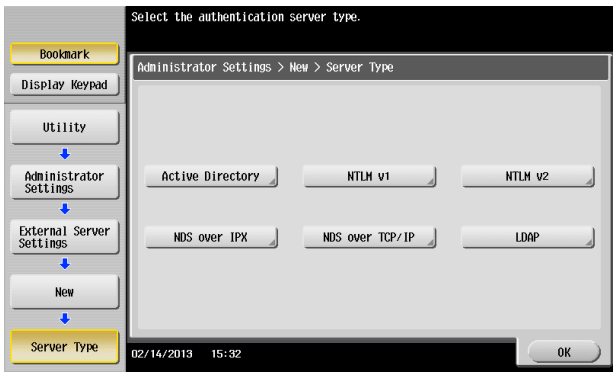
4 Touch [New].



➔ To change or delete a previously registered server, touch [Edit] or [Delete].

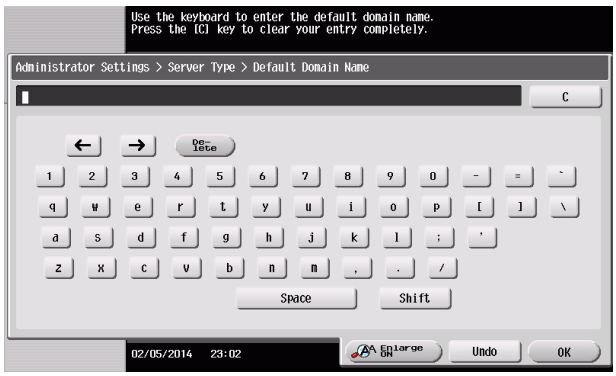
5 Touch [Server Type].

6 Touch [Active Directory].



7 Touch [Default Domain Name].

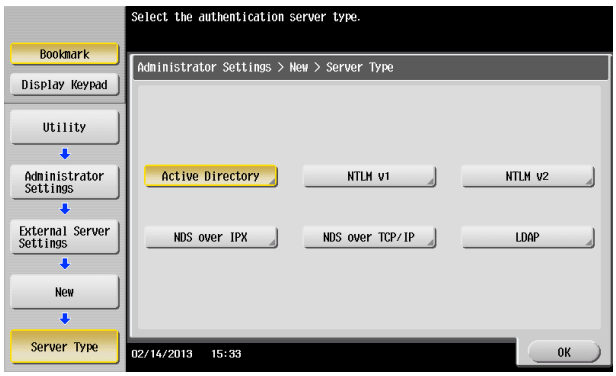
8 From the keyboard, enter the Domain Name and touch [OK].



➔ Touch [C] or touch [Undo] to clear the value entered last.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.

9 Touch [OK].

10 Touch [OK].



11 Make the necessary settings.

➔ If the Sever Name is yet to be entered, [OK] cannot be touched. Be sure to enter the Sever Name.

➔ A Sever Name that already exists cannot be redundantly registered.

12 Touch [OK].

13 Touch [Close].

➔ If two or more External Servers have been registered, select any desired server and touch [Set as Default].

2.6 ID & Print Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of the ID & Print Setting function.

ID & Print is a function to authenticate a user using a user name and password, then automatically print the print jobs saved in the ID & Print User Box of this machine, when user authentication is enabled.

NOTICE

The administrator must first make User Authentication settings before setting the ID & Print. For details of the User Authentication, see page 2-20.

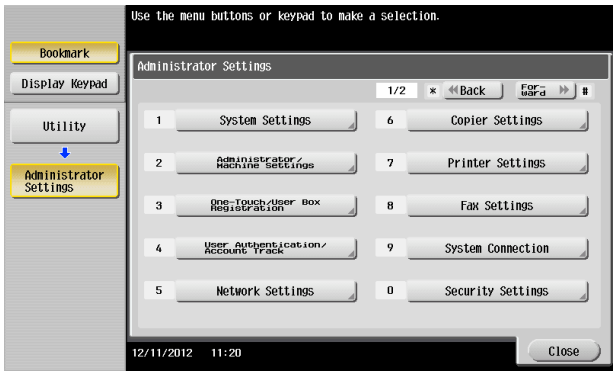
Setting ID & Print

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

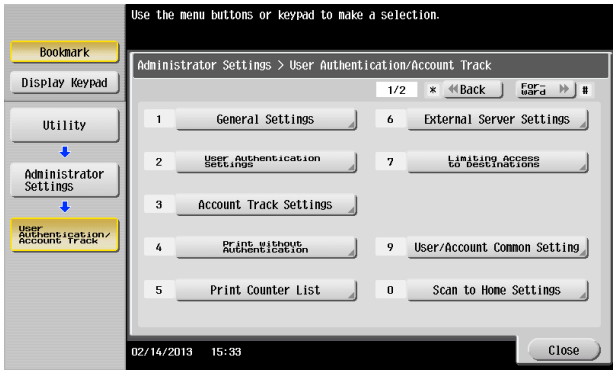
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Administrator Settings on the display from the control panel.

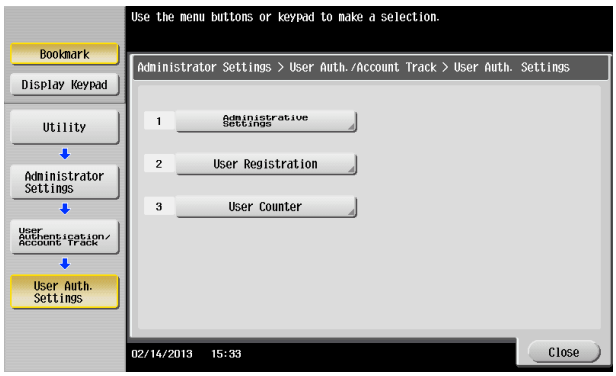
2 Touch [User Authentication/Account Track].



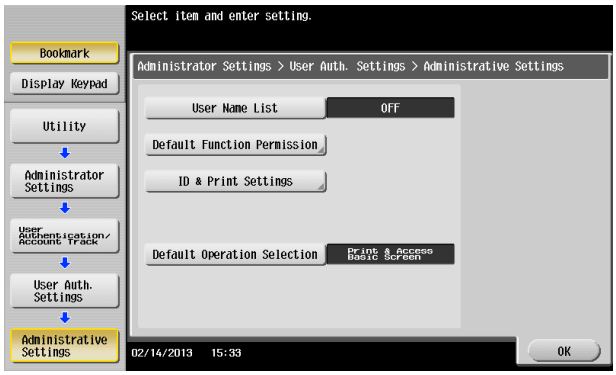
3 Touch [User Authentication Settings].



4 Touch [Administrative Settings].



5 Touch [ID & Print Settings].



6 Select [ON].

7 Touch [OK].

➔ If [ON] is set, the document is stored as ID & Print document even if [Print] is selected on the printer driver side.

➔ Even if [OFF] is set, the document is stored as ID & Print document if [ID & Print] is selected on the printer driver side.

2.7 System Auto Reset Function

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of the System Auto Reset function.

If no operations are performed for a predetermined period of time during access to the Administrator Settings or user mode (during setting of User Authentication) from the control panel, the System Auto Reset function automatically causes the user to log off from the mode.

The predetermined period of time, after which the System Auto Reset function is activated, can be selected from among nine values between 1 min. and 9 min. System Auto Reset can also be set to [OFF]. If no operations are performed for 1 min. even with System Auto Reset set to [OFF], the function causes the user to log off from the mode automatically.

Reference

- Processing of a specific job, however, takes precedence over the System Auto Reset function. That is, even if a predetermined period of time elapses during which no operations are performed, once the processing of the specific job has been started, the System Auto Reset function does not cause the user to log off from the mode. The user logs off from the mode after the lapse of a predetermined period of time after the processing of the specific job is completed.

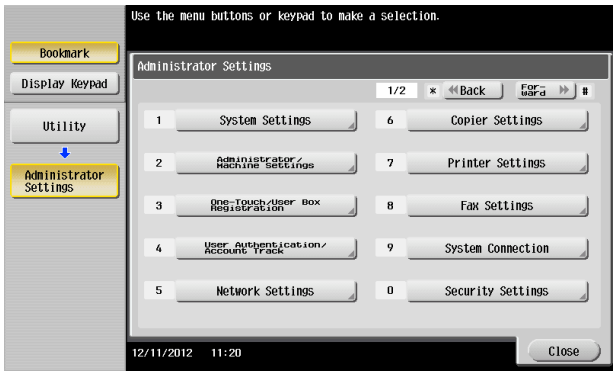
Setting the System Auto Reset function

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

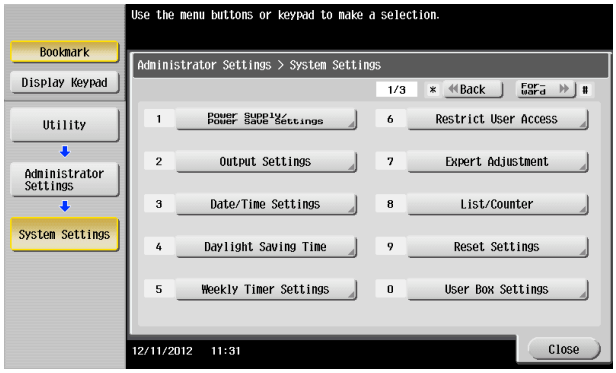
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Administrator Settings on the display from the control panel.

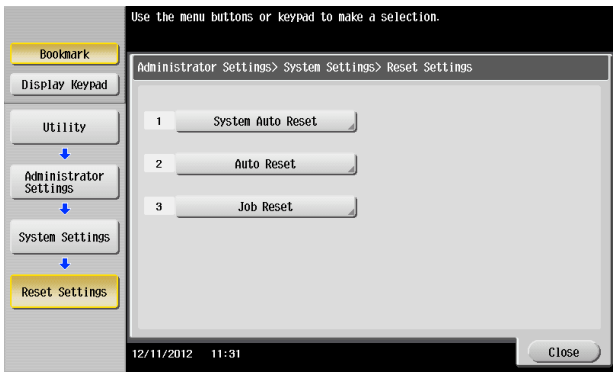
2 Touch [System Settings].



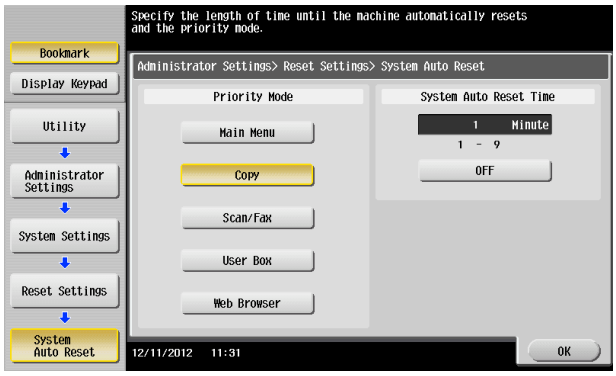
3 Touch [Reset Settings].



4 Touch [System Auto Reset].



5 Touch [C] and enter the period of time (1 min. to 9 min.) after which System Auto Reset is activated from the keypad.



➔ Touch [Display Keypad] to display the keypad.

➔ The time for System Auto Reset can be set to a value between 1 min. and 9 min., variable in 1-min. increments. An input data error message appears when any value falling outside the range of 1 to 9 min. is set. Enter the correct System Auto Reset Time.

➔ If no operations are performed for 1 min. even with System Auto Reset set to [OFF], the function is activated to cause the user to log off from the mode automatically.

➔ Touch [C] to clear all characters.

6 Touch [OK].

2.8 User Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables registration of the users who can use the machine. It also enables operations for deleting a user and changing a User Password. In PageScope Web Connection, import/export of the user registration information is enabled, allowing the backup data of the user registration information to be saved or the saved backup data to be restored.

User Registration allows the User Name, User Password, and other user information to be registered for enabling access to, or operation of, the machine. Up to 1,000 different users can be registered. User Registration allows identification and authentication of each individual user, thereby preventing unauthorized use of the machine. The User Password is controlled based on passwords that meets the Password Rules and the password entered is displayed as "*" or "●."

Reference

- If [External Server Authentication] (Active Directory) is set for the authentication method, it is not possible to make user registration or change a User Password from the control panel. To register or change a user, make the settings on the server side. If PageScope Data Administrator is used for registering user information, however, the user name must match that registered in the External Server. Further, a User Password can be set, but is not to be used for authentication.
- If [External Server Authentication] (Active Directory) is set for the authentication method and if a user not registered with this machine is authenticated through user authentication, that particular user name is automatically registered in the machine.
- If [External Server Authentication] (Active Directory) is set for the authentication method and if a user registered with this machine is authenticated through user authentication, that particular user name, along with the External Server name, is automatically registered in the machine. No two User Names registered in an External Server may be alike.
- If the user authentication method is changed between [ON (MFP)] and [External Server Authentication], the user information registered under the previous authentication method cannot be used under the new authentication method.
- If the user authentication method is to be changed, be sure first to delete all user information used under the old authentication method and then change the user authentication method as necessary. When a registered user is deleted, the Personal User Box owned by the user who has been deleted can be deleted or changed to a Public User Box.
  If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.
- If [ON (MFP)] is set for the authentication method, a specific registered user may be temporarily suspended from using the machine or a suspended user may be allowed to use the machine again. While a user is suspended from using the machine, he or she cannot log onto the machine.
- [Pause] setting for the user is disabled if [External Server Authentication] (Active Directory) is set for the authentication method.

Making user setting

<From the Control Panel>

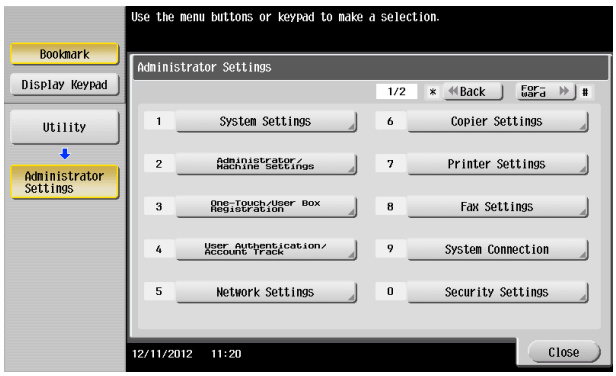
✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

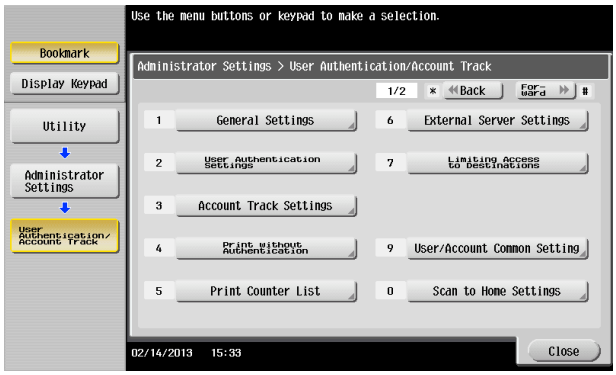
✔ If synchronization with Account Track has been set, the account should be registered in advance. For how to make the Account Track Registration, see page 2-36.

1 Call the Administrator Settings on the display from the control panel.

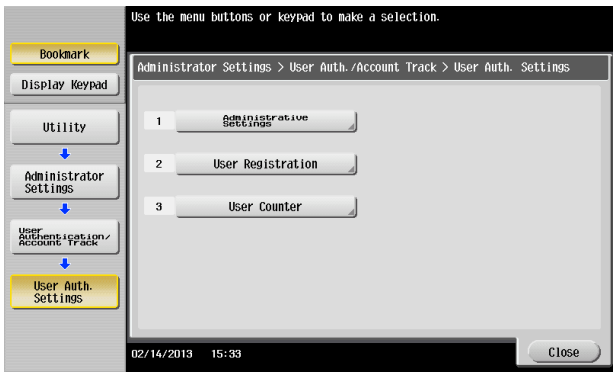
2 Touch [User Authentication/Account Track].



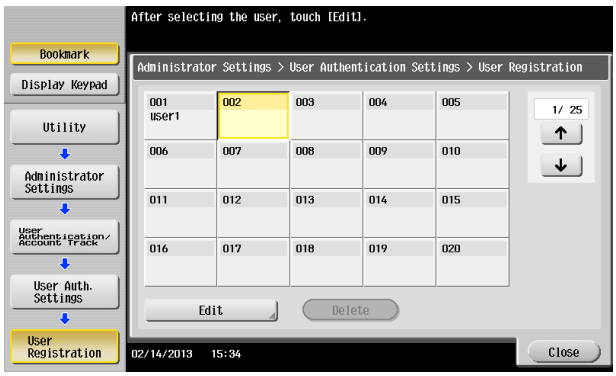
3 Touch [User Authentication Settings].



4 Touch [User Registration].



5 Select a specific User Registration key, in which no user has been registered, and touch [Edit].

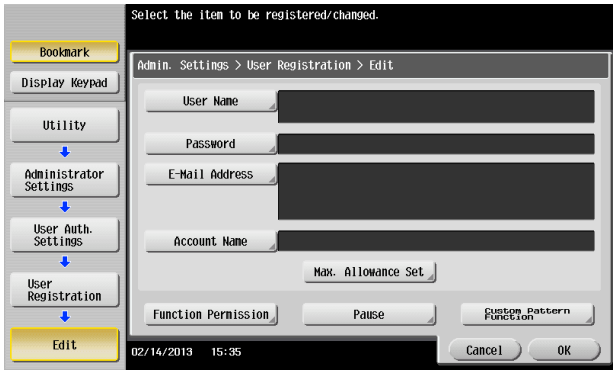


➔ To change settings for a registered user, select the registered user in question and touch [Edit].

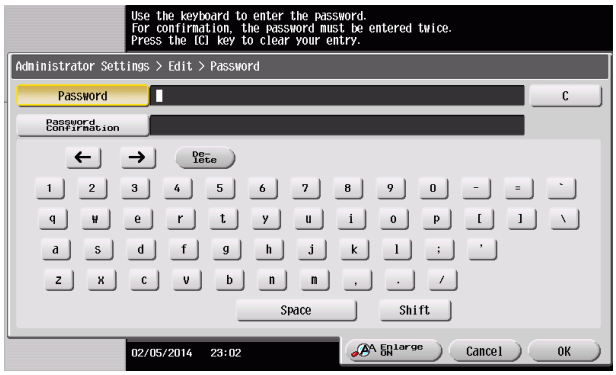
➔ To delete a registered user, select the registered user in question and touch [Delete]. The following screen appears if the user to be deleted owns a Personal User Box. Select whether to delete the Personal User Box or change it to the Public User Box.

➔ If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

6 Touch [Password].



7 From the keyboard, enter a new User Password.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



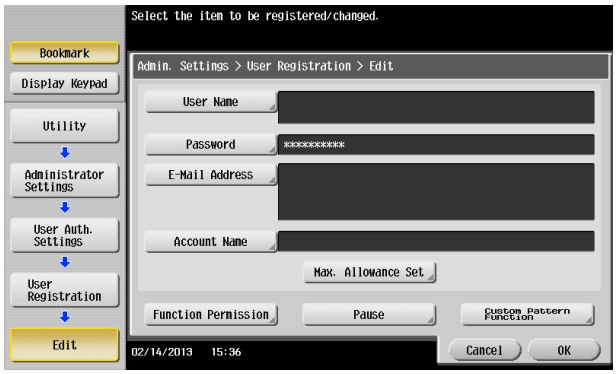
➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

8 Touch [OK].

➔ If the entered User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-11.

➔ If the entered User Password does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.

9 Touch [Account Name].



➔ If Account Name is not registered, Account Track becomes necessary even with [Synchronize] set for [Synchronize User Authentication & Account Track]. Account Track is, however, necessary only for the first time. Once any account is authenticated, that particular account is registered for Account Name. The machine can thereafter be used only through User Authentication.
It should be noted that this function is valid only through operation from the control panel of the machine. In operation from PageScope Web Connection or application software, if Account Name is not registered, you cannot log onto the mode.

➔ [Account Name] does not appear, if Account Track has not been set for the authentication method or any option other than [Synchronize] has been selected for [Synchronize User Authentication & Account Track].

10 Select the desired account.

11 Touch [OK].

12 Make the necessary settings.

➔ If the User Name is yet to be entered, [OK] cannot be touched. Be sure to enter the User Name.

➔ A User Name that already exists cannot be redundantly registered.

➔ To suspend temporarily a registered user from using the machine, touch [Pause] and select [Stop Job]. If the account to which the user belongs is temporarily suspended from using the machine, however, selecting [Continue Job] does not allow the user to use the machine.

➔ To restrict the functions the user can use, use [Function Permission] and set Allow or Restrict for each function. Setting [All Users] applies the same [Function Permission] to all users.

13 Touch [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

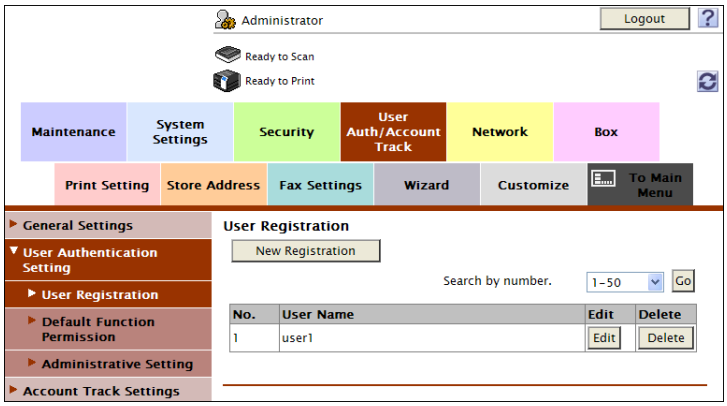
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [User Auth/Account Track] tab.

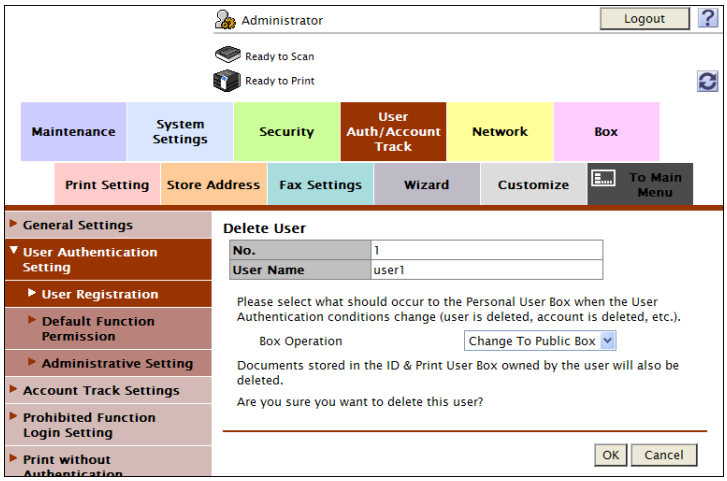
3 Click [User Authentication Setting] ▸▸ [User Registration] from the menu.

4 Click the [New Registration].



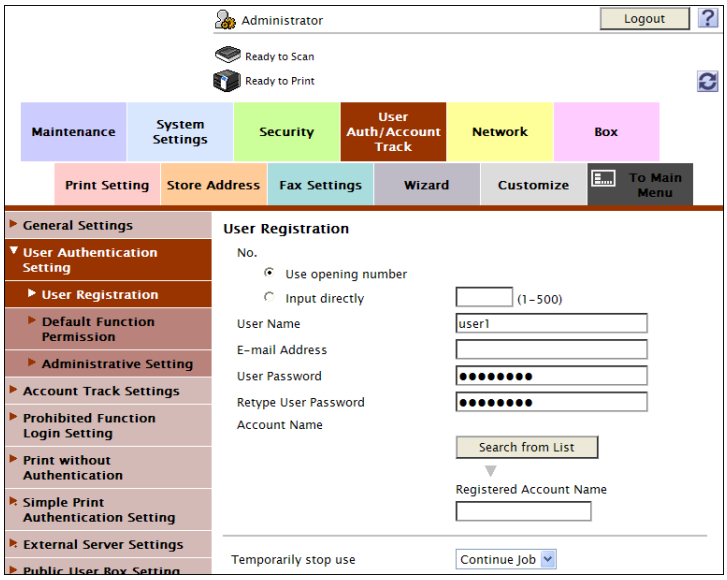
➔ Click [Edit] to change settings for a previously registered user.

➔ To delete a registered user, select the registered user in question and click [Delete]. The following screen appears if the user to be deleted owns a Personal User Box. Select whether to delete the Personal User Box or change it to the Public User Box.



➔ If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

5 Make the necessary settings.



➔ A number that already exists cannot be redundantly registered.

➔ A User Name that already exists cannot be redundantly registered.

➔ [Account Name] does not appear, if Account Track has not been set for the authentication method or any option other than [Synchronize] has been selected for [Synchronize User Authentication & Account Track].

➔ To suspend temporarily a registered user from using the machine, select [Stop Job] from the pull-down menu of [Temporarily stop use]. If the account to which the user belongs is temporarily suspended from using the machine, however, selecting [Continue Job] does not allow the user to use the machine.

➔ To restrict the functions the user can use, use [Function Permission] and set Allow or Restrict for each function.

➔ Click [Cancel] to go back to the previous screen.

6 Click [OK].

➔ If the entered User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-11.

➔ If the entered User Password does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.

7 Check the message that tells that the setting has been completed.

2.9 Account Track Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables registration of accounts, for which use of the machine is restricted. It also enables operations for deleting an account and changing an Account Password. In PageScope Web Connection, import/export of the account registration information is enabled, allowing the backup data of the account registration information to be saved or the saved backup data to be restored.

Account Track Registration allows the Account Name, Account Password, and other account information to be registered for enabling access to, or operation of, the machine. Up to 1,000 different users or accounts can be registered. The Account Password is controlled based on passwords that meets the Password Rules and the password entered is displayed as "*" or "●."

Reference

- A specific registered account may be temporarily suspended from using the machine or a suspended account may be allowed to use the machine again. While an account is suspended from using the machine, it cannot log onto the machine. If a registered account to which a particular user belongs is suspended from using the machine, that particular user is also unable to log onto the machine.
- [Pause] setting of the account is enabled even if [External Server Authentication] (Active Directory) is set for the authentication method.

Making account setting

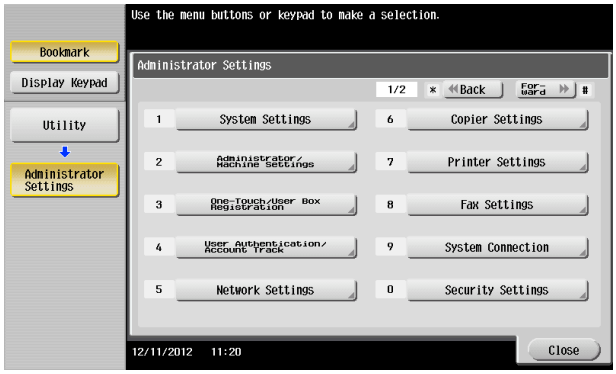
<From the Control Panel>

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

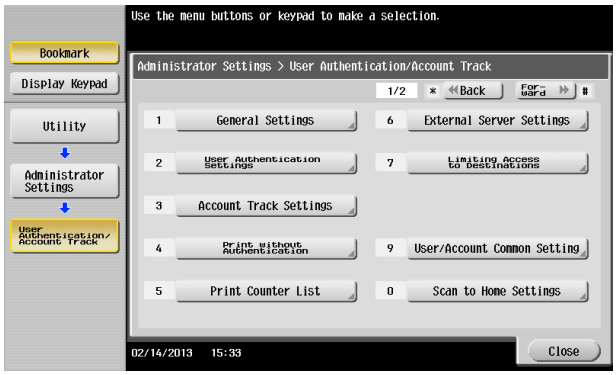
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Administrator Settings on the display from the control panel.

2 Touch [User Authentication/Account Track].

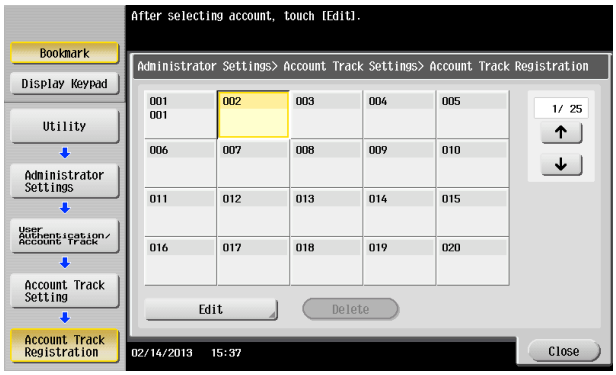


3 Touch [Account Track Settings].



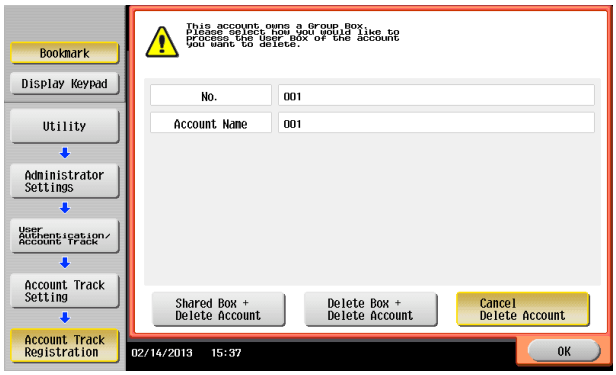
4 Touch [Account Track Registration].

5 Select a specific Account Registration key, in which no account has been registered, and touch [Edit].



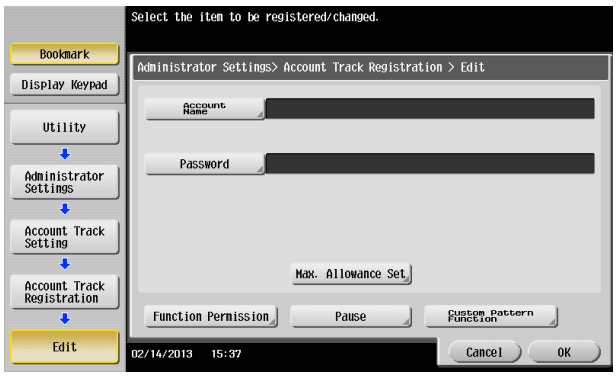
➔ To change settings for a registered account, select the registered account in question and touch [Edit].

➔ To delete a registered account, select the registered account in question and touch [Delete]. The following screen appears if the account to be deleted owns a Group User Box. Select whether to delete the Group User Box or change it to the Public User Box.

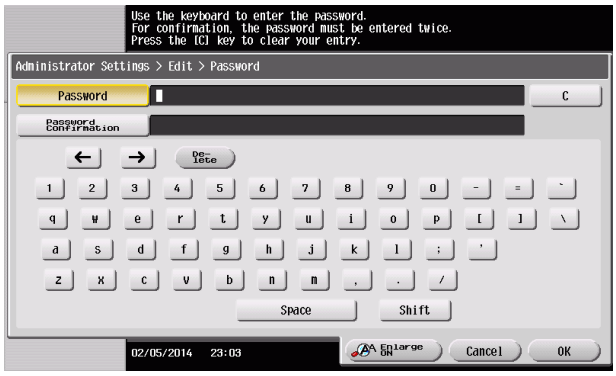

This account owns a Group Box. Please select how you would like to process the User Box of the account you want to delete.
Bookmark
Display Keypad
Utility
Administrator Settings
User Authentication/ Account Track
Account Track Setting
Account Track Registration
No. 001
Account Name 001
Shared Box + Delete Account
Delete Box + Delete Account
Cancel Delete Account
02/14/2013 15:37
OK

➔ If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

6 Touch [Password].



7 From the keyboard, enter a new Account Password.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

8 Touch [OK].

➔ If the entered Account Password does not meet the Password Rules, a message that tells that the entered Account Password cannot be used appears. Enter the correct Account Password. For details of the Password Rules, see page 1-11.
➔ If the entered Account Password does not match, a message that tells that the Account Password does not match appears. Enter the correct Account Password.

9 Make the necessary settings.

➔ If the Account Name is yet to be entered, [OK] cannot be touched. Be sure to enter the Account Name.
➔ An Account Name that already exists cannot be redundantly registered.
➔ To suspend temporarily a registered account from using the machine, touch [Pause] and select [Stop Job]. If [Stop Job] is selected, a user who belongs to that particular account is also temporarily suspended from using the machine.
➔ To restrict the functions the account can use, use [Function Permission] and set Allow or Restrict for each function. Setting [All Accounts] applies the same [Function Permission] to all accounts.

10 Touch [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

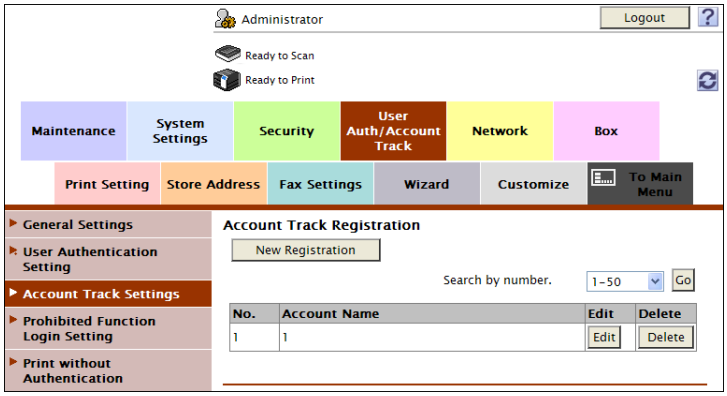
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [User Auth/Account Track] tab.

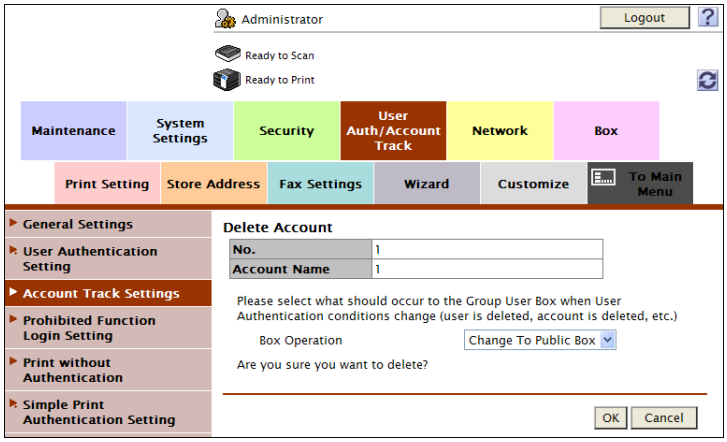
3 Click [Account Track Settings] from the menu.

4 Click [New Registration].



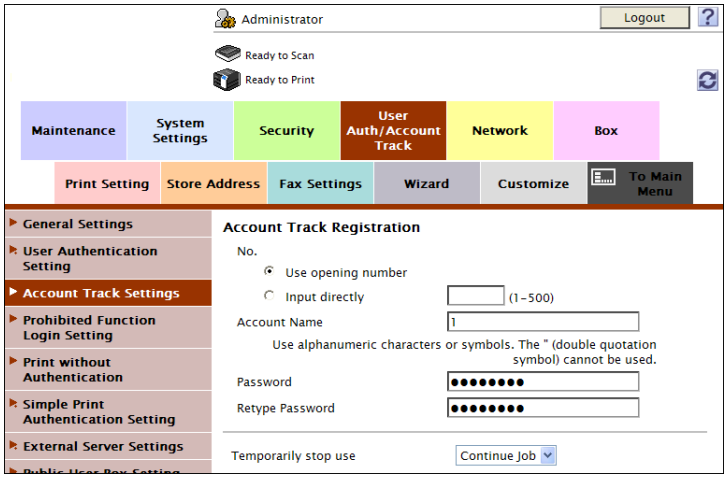
➔ Click [Edit] to change settings for a previously registered account.

➔ To delete a registered account, select the registered account in question and click [Delete]. The following screen appears if the account to be deleted owns a Group User Box. Select whether to delete the Group User Box or change it to the Public User Box.



➔ If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

5 Make the necessary settings.



➔ A number that already exists cannot be redundantly registered.

➔ An Account Name that already exists cannot be redundantly registered.

➔ To suspend temporarily a registered account from using the machine, select [Stop Job] from the pull-down menu of [Temporarily stop use]. If [Stop Job] is selected, a user who belongs to that particular account is also temporarily suspended from using the machine.

➔ To restrict the functions the account can use, use [Function Permission] and set Allow or Restrict for each function.

➔ Click [Cancel] to go back to the previous screen.

6 Click [OK].

➔ If the entered Account Password does not meet the Password Rules, a message that tells that the entered Account Password cannot be used appears. Enter the correct Account Password. For details of the Password Rules, see page 1-11.

➔ If the entered Account Password does not match, a message that tells that the Account Password does not match appears. Enter the correct Account Password.

7 Check the message that tells that the setting has been completed.

2.10 User Box Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables the User Box. It also allows the User Box Password and user and account attributes to be changed.

User Box prepares a User Box in the HDD as a space for saving image files. Up to 1,000 Personal, Public and Group User Boxes can be registered. The Public User Box Password is controlled based on passwords that meets the Password Rules and the password entered is displayed as "*" or "●."

The term "user attributes" is a generic name used to refer to Owner Change and User Box Type.

The term "account attributes" is a generic name used to refer to Owner Change and Account Box Type.

NOTICE

Setting the Memory RX function allows a received fax to be stored in the box without its being printed. Because the received faxes are forcibly stored in this box, this will prevent important faxes from being stolen or lost and therefore enhance security. For details, see page 2-52.

Reference

- If [External Server Authentication] (Active Directory) is set for the authentication method, the same Personal User Box name as that registered with the machine can be created and registered along with the External Server name. No two Personal User Box names registered in an External Server may be alike.
- If a document is saved in the Copy mode, Fax/Scan mode, or User Box mode selected from the control panel, or from an external memory, by specifying a User Box number that has not been registered, a Personal User Box owned by the user who logged on through User Authentication or a Group User Box owned by the account to which the user who logged on through User Authentication belongs is automatically created. No Public User Boxes are automatically created.
- When a document is saved in a box with a box number yet to be registered specified from the PC, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.
- To use the external memory function, settings must be made by the administrator of the machine. For details, refer to the User's Guide furnished with the machine.

2.10.1 Setting the User Box

<From the Control Panel>

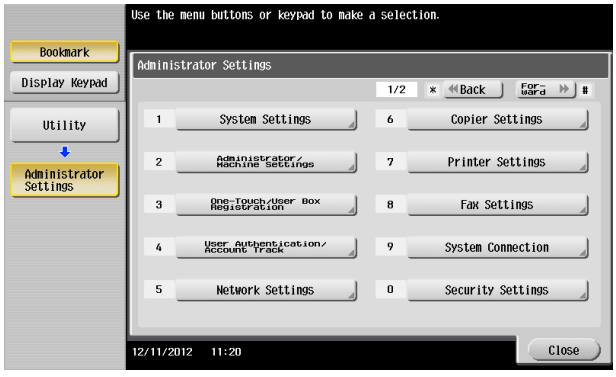
✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

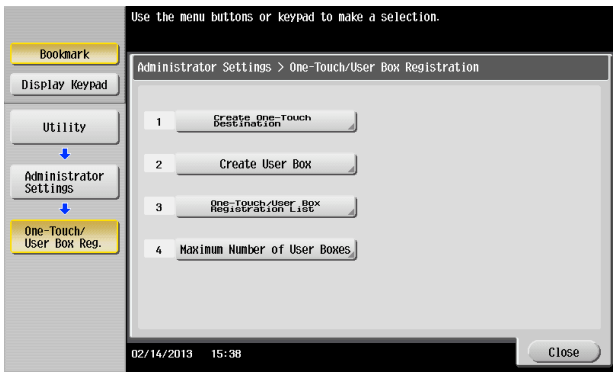
✔ For the procedure to change the user attributes, account attributes, and User Box Password, see page 2-47.

1 Call the Administrator Settings on the display from the control panel.

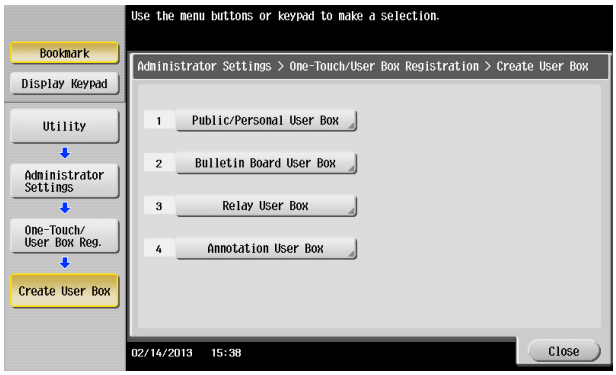
2 Touch [One-Touch/User Box Registration].



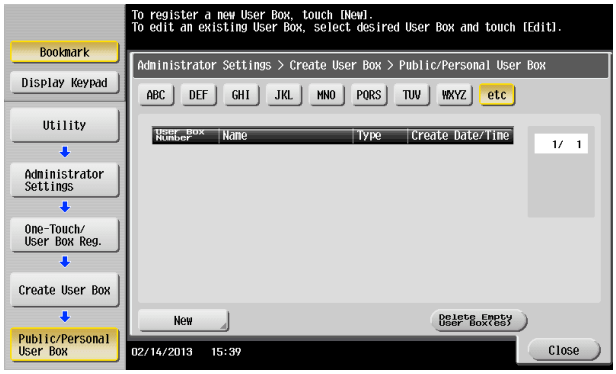
3 Touch [Create User Box].



4 Touch [Public/Personal User Box].

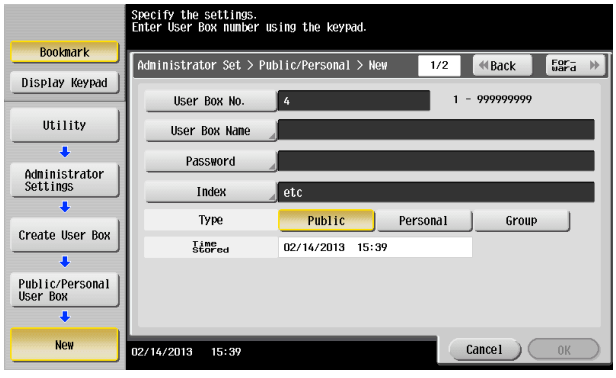


5 Touch [New].

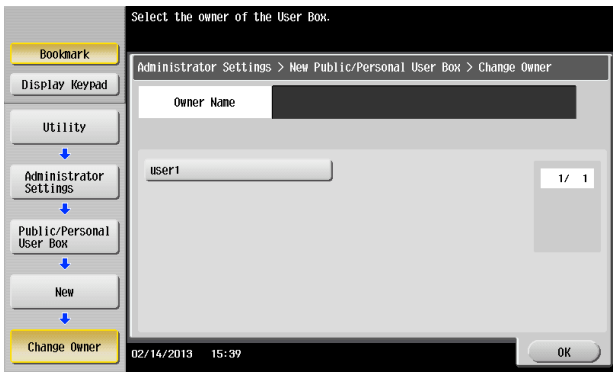


➔ To delete a User Box, select the desired user box key and touch [Delete]. A confirmation message appears. Select [Yes] and touch [OK] to delete the specified User Box.

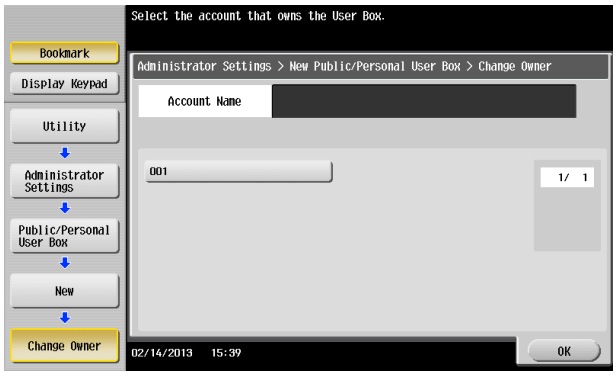
6 Select the User Box Type.



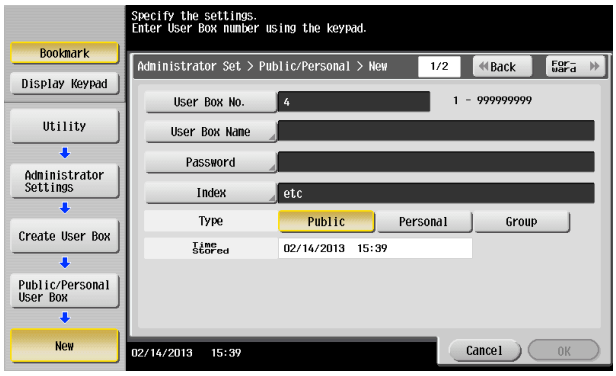
➔ When [Personal] is selected, [Change Owner] is displayed. Then, select the desired owner name.



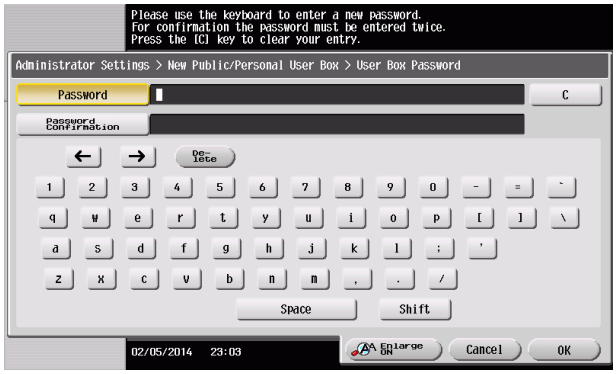
➔ When [Group] is selected, [Change Account Name] is displayed. Then, select the desired account name.



7 Touch [Password].



8 Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



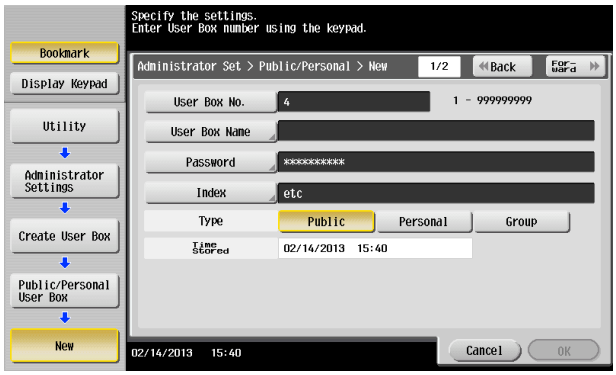
➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

9 Touch [OK].

➔ If the User Box Type is set to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.
➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

10 Make the necessary settings.



➔ A User Box No. that already exists cannot be redundantly registered.
➔ If no User Box Name has been registered, [OK] cannot be touched. Be sure to register the User Box Name.

11 Touch [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

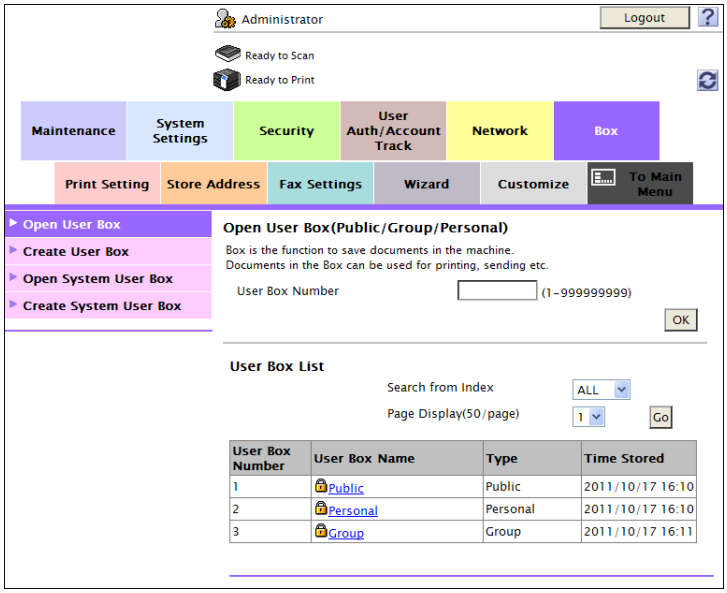
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

✔ For the procedure to change the user attributes, account attributes and User Box Password, see page 2-47.

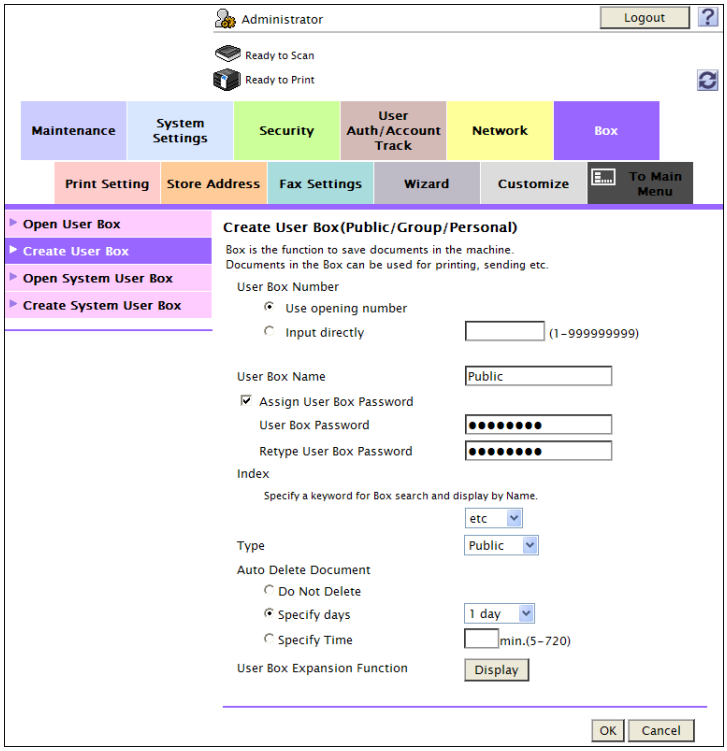
1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Box] tab.

3 Click [Create User Box] from the menu.



4 Make the necessary settings.



➔ Be sure to enter the User Box Number, User Box Name, User Box Password, and Retype User Box Password.

➔ A User Box Number that already exists cannot be redundantly registered.

➔ If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.

➔ If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.

5 Click [OK].

➔ If the User Box Type is set to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.

➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

➔ If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.

➔ If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.

➔ If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.

➔ If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.

2.10.2 Changing the user/account attributes and box password

The administrator of the machine can change the box type of the box previously registered. For the Personal User Box, the owner user can be changed, and for the Group User Box, the owner account can be changed.

<From the Control Panel>

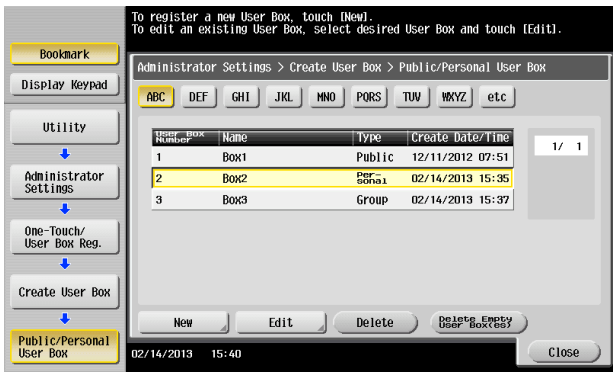
✔ For the procedure to call the User Box setting screen on the display, see steps 1 through 4 of page 2-41.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

✔ Changing the box type to [Public] nullifies the setting of the owner user or owner account.

1 Call the User Box setting screen on the display from the control panel.

2 Select the desired User Box key and touch [Edit].

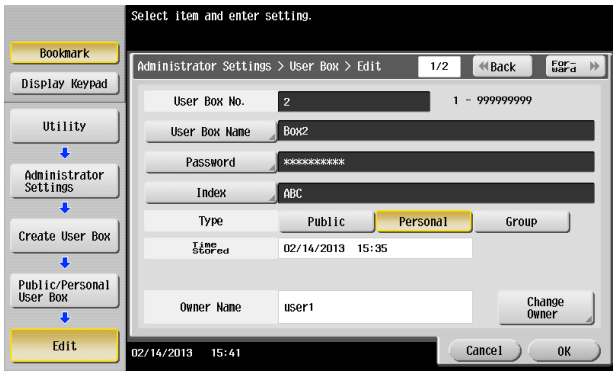


➔ To change the User Box Type, perform steps 3 through 6.

➔ To change the owner user or owner account, perform steps 4 through 6.

➔ To change the User Box Password, go to step 7.

3 Select the User Box Type.

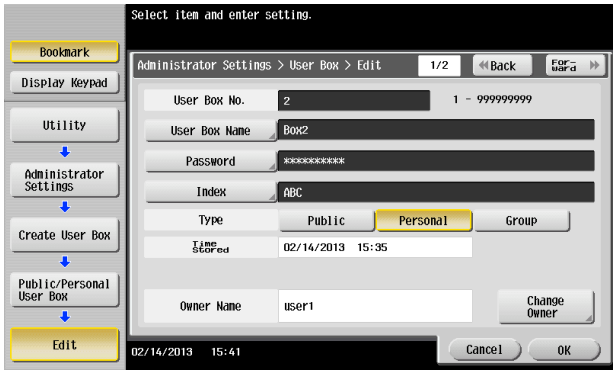


➔ [Change Owner] appears if the Box Type is changed to [Personal]. Select the desired owner name.

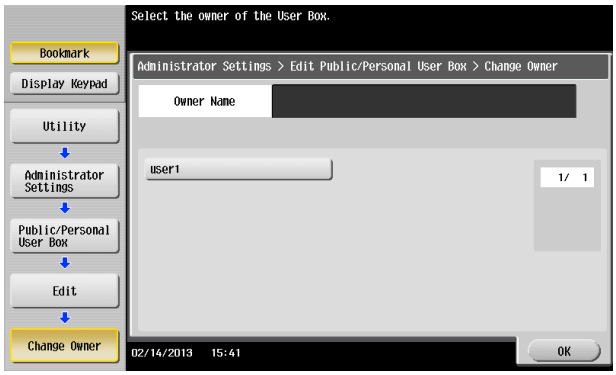
➔ [Change Account Name] appears if the Box Type is changed to [Group]. Select the desired account name.

➔ If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.

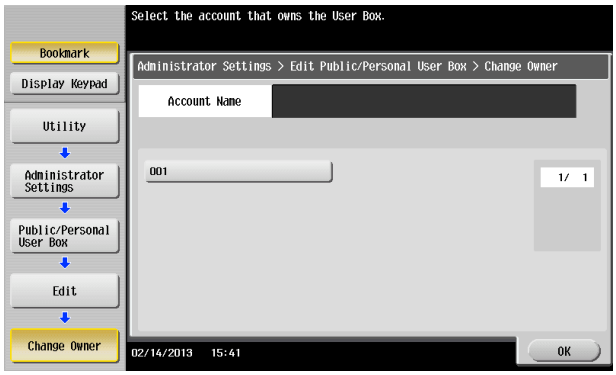
4 Touch [Change Owner] if the Box Type is [Personal] and touch [Change Account Name] if the Box Type is [Group].



5 For [Change Owner], select the desired owner name.



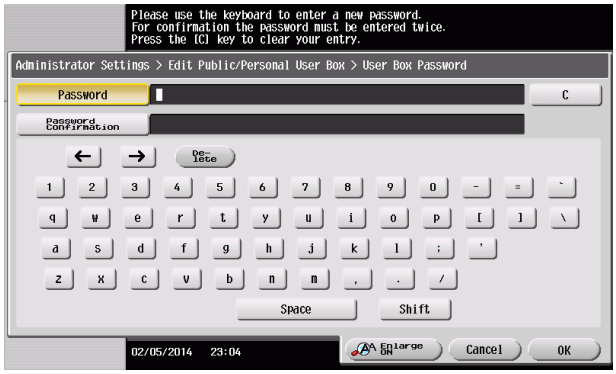
➔ For [Change Account Name], select the desired account name.



6 Touch [OK].

7 Touch [Password].

8 Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

9 Touch [OK].

➔ If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.
➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

10 Touch [OK].

<From PageScope Web Connection>

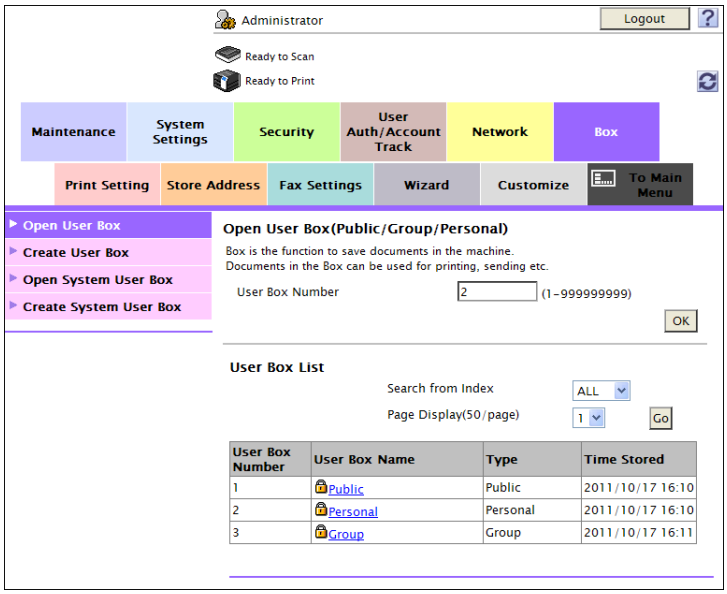
✔ For the procedure to access the Admin Mode, see page 2-2.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

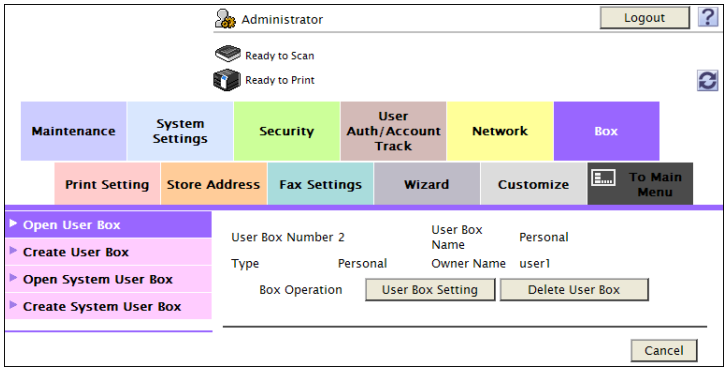
1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Box] tab.

3 Enter the target box number and click [OK], or select the target box from the box list.



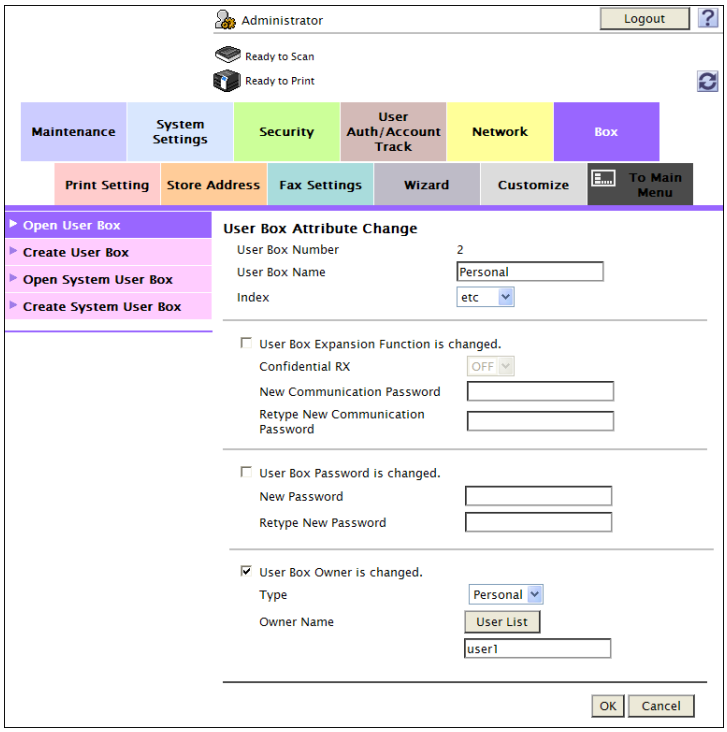
4 Click [User Box Setting].



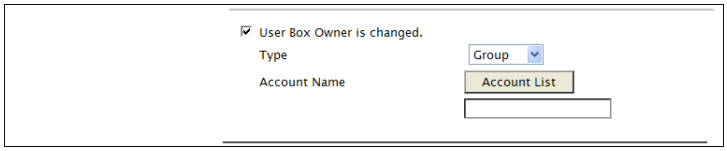
➔ Go to step 6 to change the User Box Password.

➔ To delete a User Box, click [Delete User Box]. A confirmation message appears. Click [OK] to delete the specified User Box.

5 Click the "User Box Owner is changed." check box and change the user attributes of the box.



➔ The following screen appears if the account attributes are to be changed.



➔ If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.

➔ If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.

➔ If the "User Box Owner is changed." check box is not clicked, the changes made will not be validated. If the changes need to be made, make sure that the "User Box Owner is changed." check box has been clicked.

➔ To change the User Box Type, click the Type pull-down menu and select the desired box type.

6 Click the "User Box Password is changed." check box and enter the User Box Password.

7 Click [OK].

➔ If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.

➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

➔ If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.

➔ If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.

➔ If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.

➔ If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.

2.10.3 Setting Memory RX

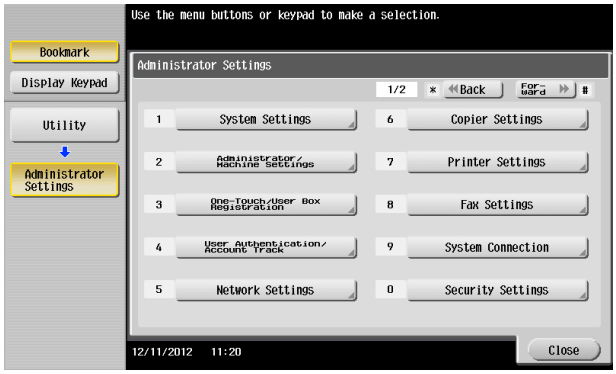
<From the Control Panel>

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

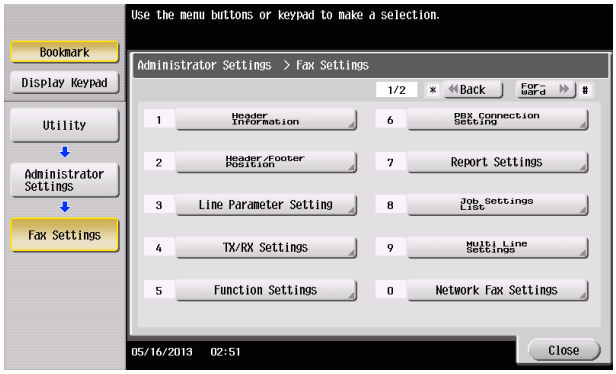
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Administrator Settings on the display from the control panel.

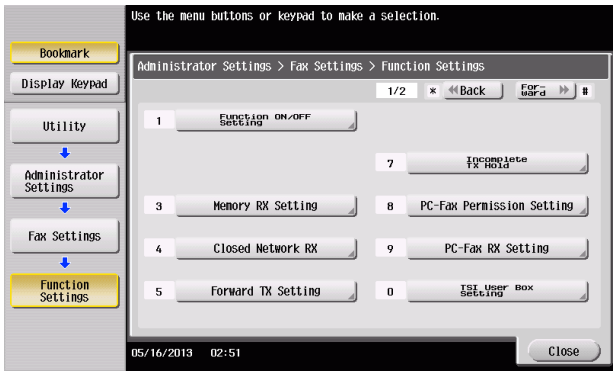
2 Touch [Fax Settings].



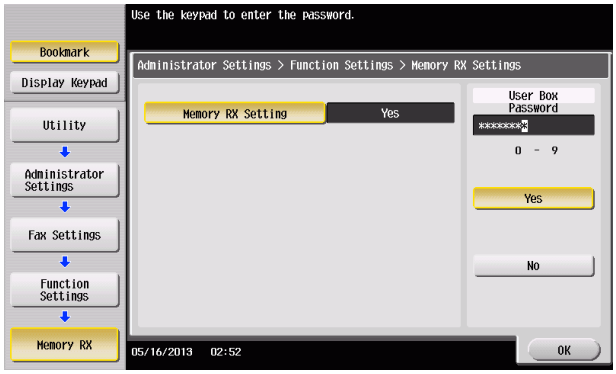
3 Touch [Function Settings].



4 Touch [Memory RX Setting].



5 Touch [Memory RX Setting]. Then, select [Yes] and enter the Memory RX User Box Password consisting of eight characters from the ten-key pad.



➔ Touch [Display Keypad] to display the keypad.

➔ Make sure that the Memory RX User Box Password consists of eight characters.

6 Touch [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

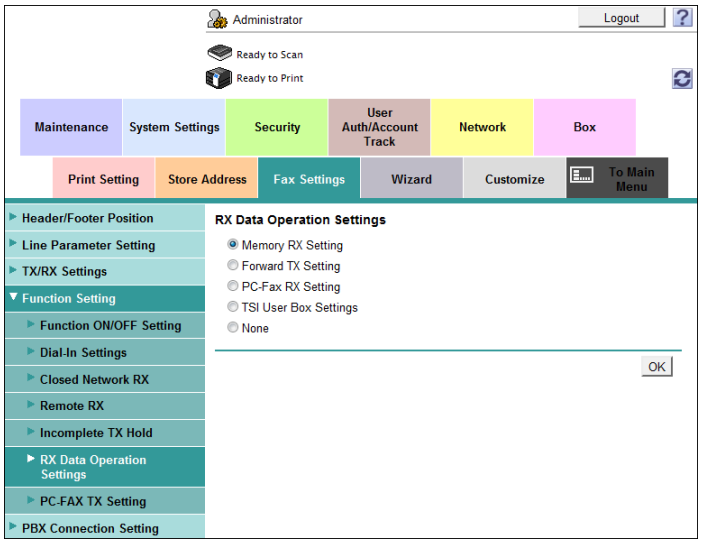
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

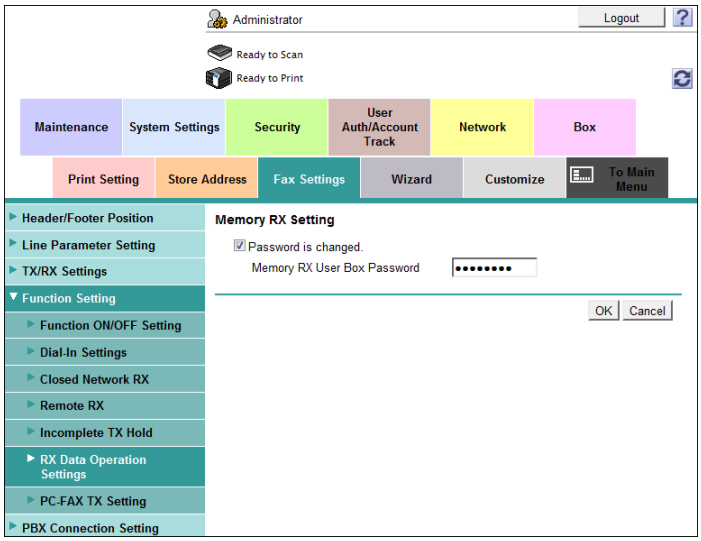
2 Click the [Fax Settings] tab.

3 Click [Function Setting] ▸▸ [RX Data Operation Settings] from the menu.

4 Select [Memory RX Setting] and click [OK].



5 Select the check box under [Password is changed] and set the Memory RX User Box Password that should consist of eight characters.



➔ Make sure that the Memory RX User Box Password consists of eight characters.

6 Click [OK].

2.11 Changing the Administrator Password

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables the operation of changing the Administrator Password required for accessing the Administrator Settings.

The Administrator Password entered for the authentication purpose appears as "*" on the display.

Changing the Administrator Password

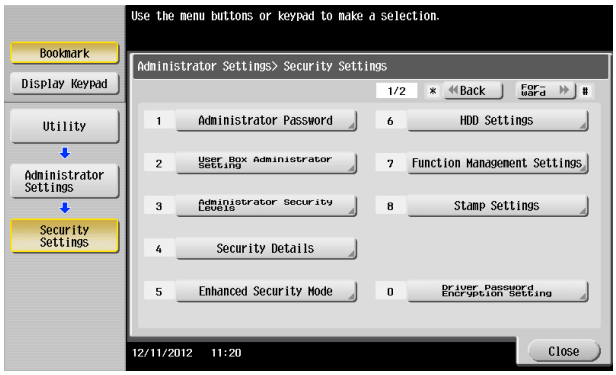
<From the Control Panel>

✔ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-13.

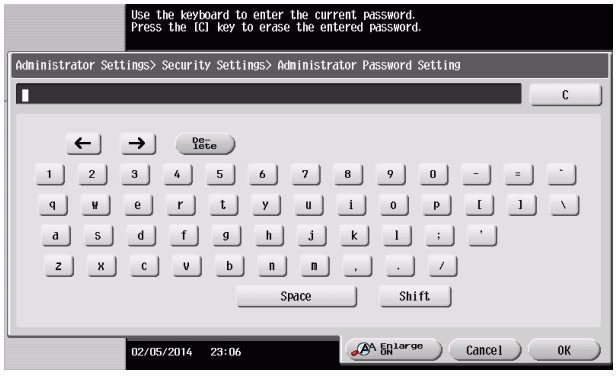
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Security Settings screen on the display from the control panel.

2 Touch [Administrator Password].



3 Enter the currently set Administrator Password from the keyboard.



➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the Security Settings screen.

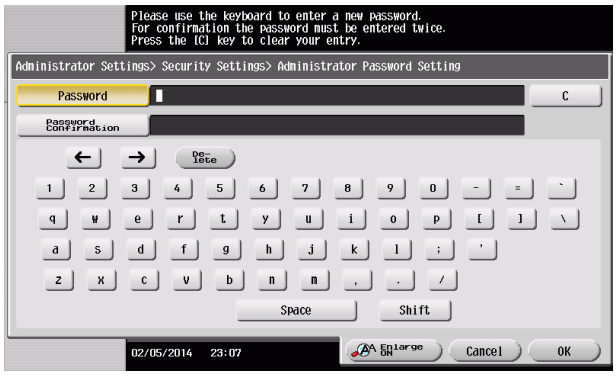
4 Touch [OK].

➔ If a wrong Administrator Password is entered, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the Utility screen appears and the machine is set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it

off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

5 Enter the new Administrator Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the Security Settings screen.

6 Touch [OK].

➔ If the entered Administrator Password does not meet the Password Rules, a message that tells that the entered Administrator Password cannot be used appears. Enter the correct Administrator Password. For details of the Password Rules, see page 1-11.
➔ If the entered Administrator Password does not match, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

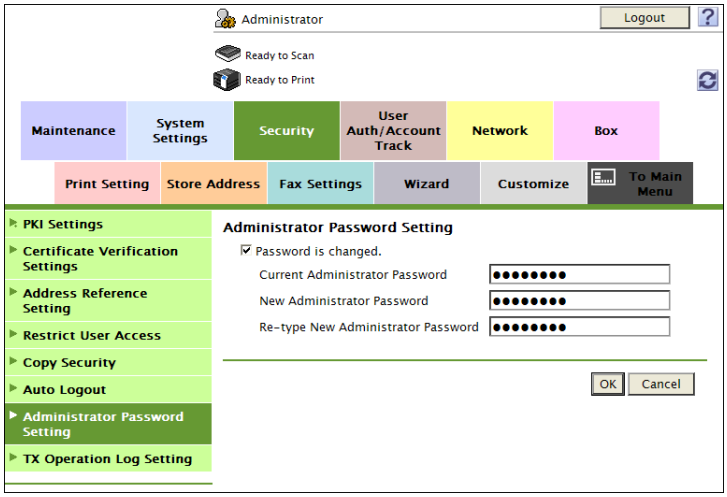
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Security] tab.

3 Click [Administrator Password Setting] from the menu.

4 Select the "Password is changed" check box. Enter the currently registered Administrator Password and a new Administrator Password. Then, to make sure that you have entered the correct new password, enter the new Administrator Password once again.



5 Click [OK].

➔ If a wrong Administrator Password is entered in the "Current Administrator Password" box, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the Utility screen appears and the machine is set into an access lock state.
To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

➔ If the entered Administrator Password in the "New Administrator Password" box does not meet the Password Rules, a message that tells that the entered Administrator Password cannot be used appears. Enter the correct Administrator Password. For details of the Password Rules, see page 1-11.

➔ If the entered Administrator Password in the "New Administrator Password" box and "Re-type New Administrator Password" box does not match, a message that tells that the Administrator Password does not match appears. Enter the correct Administrator Password.

6 Click [OK].

2.12 Protecting Data in the HDD

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables the operation for setting and changing the Encryption Key. The machine also enables the Overwrite HDD Data function.

By setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. The Encryption Key entered is displayed as "*."

NOTICE

If the HDD develops a fault, call your Service Representative.

Reference

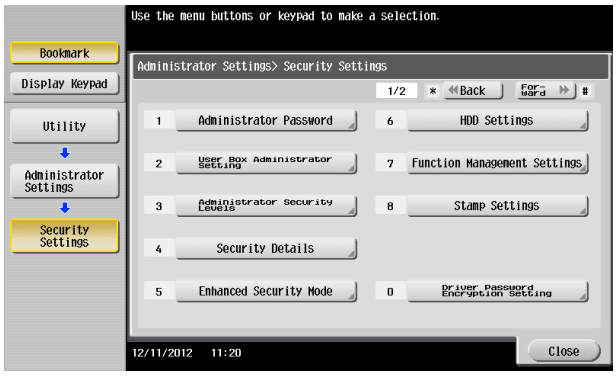
- When an Encryption Key (encryption word) is set using HDD Encryption Setting, an Encryption Key with a key length of 256 bits is generated. The generated encryption key is used to encrypt or decrypt data through AES encryption algorithm.

2.12.1 Setting the Encryption Key (encryption word)

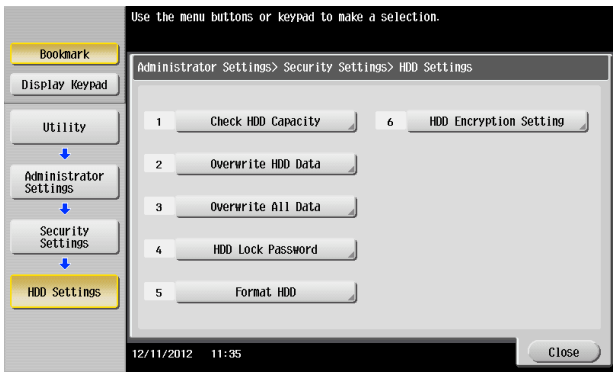
- ✔ For the procedure to call the Security Settings screen on the display, see steps 1 and 2 of page 2-13.
- ✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✔ To prevent data from leaking as a result of reinstallation of the HDD on another machine, a unique value that varies from one machine to another must be set for the encryption key.
- ✔ Do not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the Encryption Key. Try to change the Encryption Key at regular intervals.
- ✔ Make sure that nobody but the administrator of the machine comes to know the Encryption Key.
- ✔ If only the Encryption Key is to be set while the machine is being used without setting the Encryption Key, the Service Engineer must perform some setting procedures in advance. For details, contact your Service Representative.
- ✔ To edit/release the Encryption Key, see page 2-62. Do not release the Encryption Key when the Enhanced Security Mode is set to [ON]. Releasing the Encryption Key will cancel the Enhanced Security Mode.
- ✔ Executing HDD Format erases data in the HDD. It is recommended that important data should be saved in a backup medium in advance. Execution of HDD Format will also reset the setting values of different functions to the default values. Set the Enhanced Security Mode to [ON] again. For the functions whose settings are reset to the default values, see page 2-10.

1 Call the Security Settings screen on the display from the control panel.

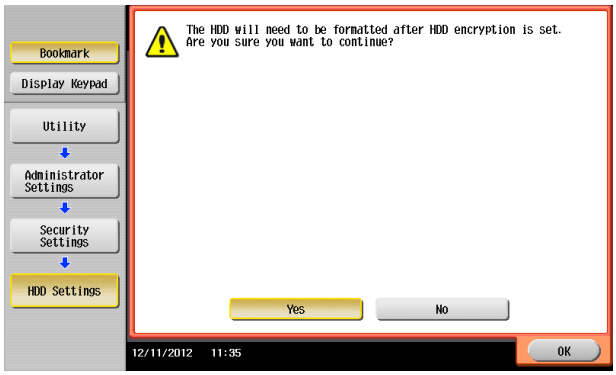
2 Touch [HDD Settings].



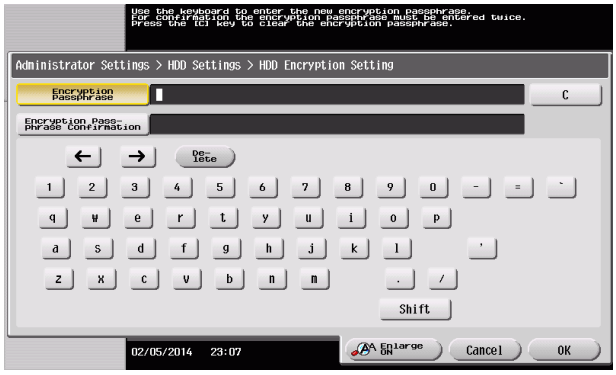
3 Touch [HDD Encryption Setting].



4 A confirmation message appears. Select [Yes] and touch [OK].



5 Enter the new 20 characters Encryption Key from the keyboard.
To prevent entry of a wrong Encryption Key, enter the Encryption Key again in [Encryption Passphrase Confirmation].

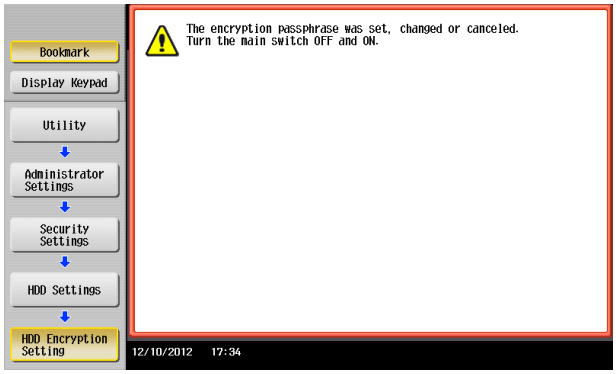


➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the HDD Settings screen.

6 Touch [OK].

➔ If the entered Encryption Key does not meet the Password Rules, a message that tells that the entered Encryption Key cannot be used appears. Enter the correct Encryption Key. For details of the Password Rules, see page 1-11.
➔ If the entered Encryption Key does not match, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

7 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



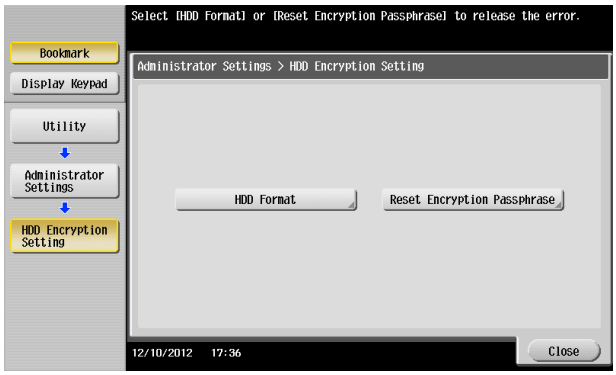
➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

8 The following screen appears after the machine has been restarted.

9 Call the Administrator Settings on the display from the control panel.

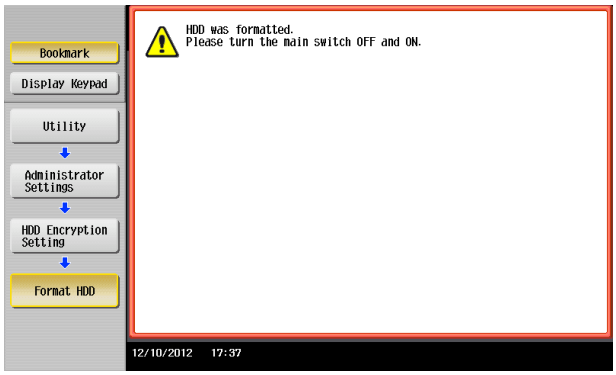
➔ For the procedure to call the Administrator Settings on the display, see page 2-2.

10 Touch [HDD Format].



11 A confirmation message appears. Select [Yes] and touch [OK].

12 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

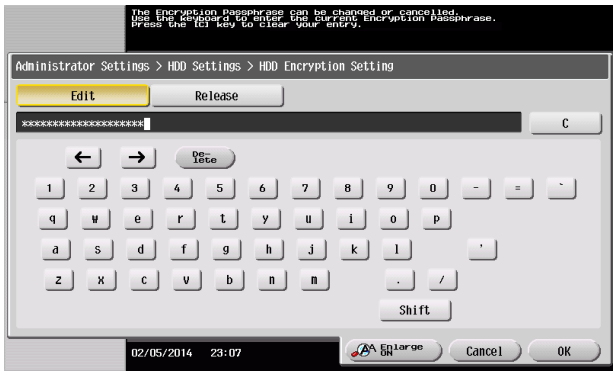
2.12.2 Changing the Encryption Key

✔ For the procedure to call the Encryption Key entry screen on the display, see steps 1 through 4 of page 2-58.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Encryption Key entry screen on the display from the control panel.

2 Enter the currently registered 20 characters Encryption Key from the keyboard.



➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.

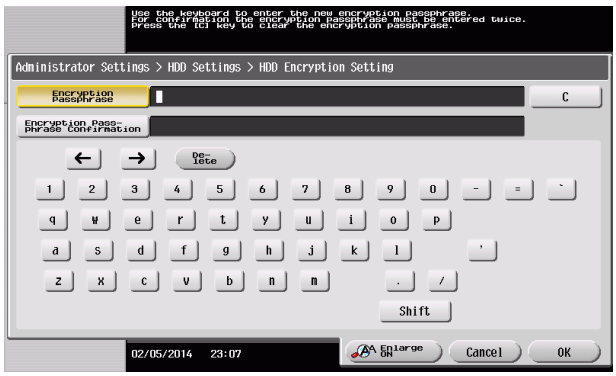
➔ Touch [Cancel] to go back to the HDD Settings screen.

3 Select [Edit] and touch [OK].

➔ If a wrong Encryption Key is entered, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

➔ Releasing the Encryption Key by selecting [Release] will cancel the Enhanced Security Mode.

4 Enter the new 20 characters Encryption Key from the keyboard.
To prevent entry of a wrong Encryption Key, enter the Encryption Key again in [Encryption Passphrase Confirmation].



➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.

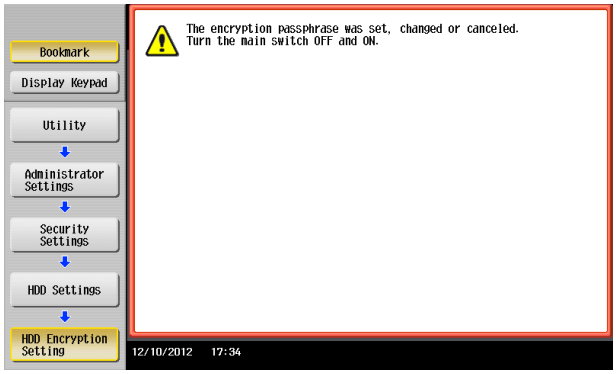
➔ Touch [Cancel] to go back to the HDD Settings screen.

5 Touch [OK].

➔ If the entered Encryption Key does not meet the Password Rules, a message that tells that the entered Encryption Key cannot be used appears. Enter the correct Encryption Key. For details of the Password Rules, see page 1-11.

➔ If the entered Encryption Key does not match, a message that tells that the Encryption Key does not match appears. Enter the correct Encryption Key.

6 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.



➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

2.12.3 Setting the Overwrite HDD Data

Setting the Overwrite HDD Data function allows data stored in the HDD to be deleted at such timing as the end of the print cycle by writing specific data over the data that is no longer required. By deleting residual data that is no longer necessary, data leakage can be prevented from occurring.

The following types of data are subject to the Overwrite HDD Data function:

- Copy, scan, print, or fax job data that is no longer necessary
- PC print job data (direct print, PS print) that is no longer necessary
- Data that is no longer necessary as a result of the data being specified to be deleted

Data stored in the HDD is to be deleted at the following timing:

- At the end (including an end as a result of cancellation) of a copy, scan, print, or fax job performed by a user who has been authenticated by User Authentication
- A job is deleted by the administrator or a user (who has been authenticated by User Authentication)
- A document in a Box is deleted by the administrator or a user (who has been authenticated by User Authentication)
- A document is deleted in a Box through Delete User Box
- A document is automatically deleted after the lapse of a predetermined period of time set in the machine *

*: The machine offers the following types of automatic box document deleting functions based on a predetermined period of time set in it.

<Administrator>

- To be set through [Utility] ▸▸ [Administrator Settings] ▸▸ [System Settings] ▸▸ [User Box Settings] ▸▸ [Document Delete Time Setting].
- To be set through [Utility] ▸▸ [Administrator Settings] ▸▸ [System Settings] ▸▸ [User Box Settings] ▸▸ [Auto Delete Secure Document].
- To be set through [Utility] ▸▸ [Administrator Settings] ▸▸ [System Settings] ▸▸ [User Box Settings] ▸▸ [ID & Print Delete Time].

<User>

- To be set through [Utility] ▸▸ [One-Touch/User Box Registration] ▸▸ [Create User Box] ▸▸ [Public/Personal User Box] ▸▸ [New] ▸▸ [Forward] ▸▸ [Auto Document Delete Time].
  Time to delete documents automatically cannot be set by the user, if [Yes] is set in [Utility] ▸▸ [Administrator Settings] ▸▸ [System Settings] ▸▸ [User Box Settings] ▸▸ [Document Delete Time Setting].

Reference

- If a job being processed is abnormally terminated, the residual data is deleted through Overwrite HDD Data.
- If the machine is turned off during an Overwrite HDD Data sequence, the Overwrite HDD Data sequence is resumed automatically after the machine is turned on again.
- If an Overwrite HDD Data sequence being performed is interrupted by, for example, a fault, a response is detected at 30-sec. intervals and the Overwrite HDD Data sequence, if found interrupted, is resumed automatically.

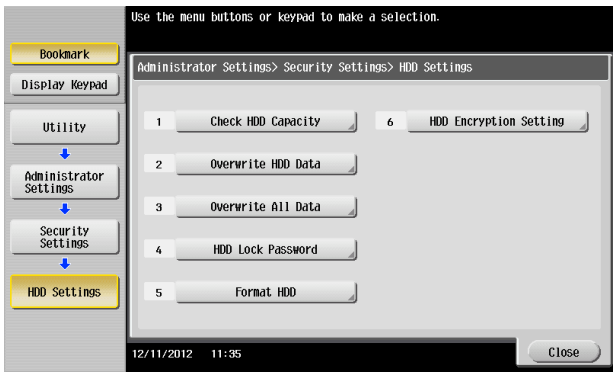
✔ For the procedure to call the HDD Settings screen on the display, see steps 1 and 2 of page 2-58.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

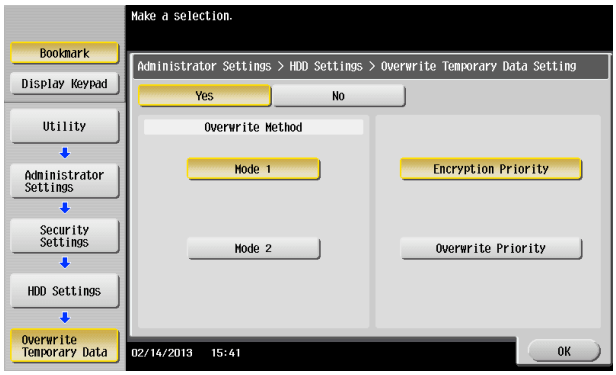
✔ Executing HDD Format erases data in the HDD. It is recommended that important data should be saved in a backup medium in advance. Execution of HDD Format will also reset the setting values of different functions to the default values. Set the Enhanced Security Mode to [ON] again. For the functions whose settings are reset to the default values, see page 2-10.

1 Call the HDD Settings screen on the display from the control panel.

2 Touch [Overwrite HDD Data].



3 Select [Yes] and then select [Mode 1] or [Mode 2].



Item	Description
[Mode 1]	Overwritten with "0x00"
[Mode 2]	Overwritten with "0x00" ▸▸ Overwritten with "0xff" ▸▸ Overwritten with letter "a" (0x61) ▸▸ Verified

➔ [No] is the default setting.

4 Touch [OK].

2.13 Overwrite All Data Function

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables setting of the operation of the Overwrite All Data function.

When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the memory area on the MFP board and the SSD board to factory settings, preventing data from leaking. For details of items that are cleared by the Overwrite All Data function, see page 1-14.

The HDD Overwrite Method offers the choice of eight different modes, [Mode 1] through [Mode 8]. Overwrite All Data takes about less than one hour in [Mode 1] at the minimum and about 9 hours in [Mode 8] at the maximum.

Mode	Description
Mode 1	Overwrites once with "0x00."
Mode 2	Overwrites with "random numbers" ▸▸ "random numbers" ▸▸ "0x00."
Mode 3	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "random numbers" ▸▸ verifies.
Mode 4	Overwrites with "random numbers" ▸▸ "0x00" ▸▸ "0xff."
Mode 5	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff."
Mode 6	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "random numbers."
Mode 7	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0xaa."
Mode 8	Overwrites with "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0x00" ▸▸ "0xff" ▸▸ "0xaa" ▸▸ verifies.

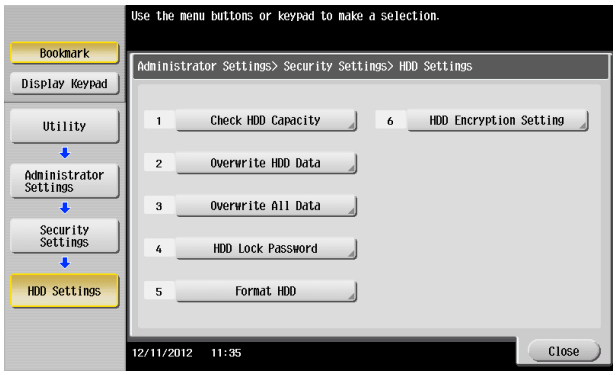
Setting the Overwrite All Data function

✔ For the procedure to call the HDD Settings screen on the display, see steps 1 and 2 of page 2-58.

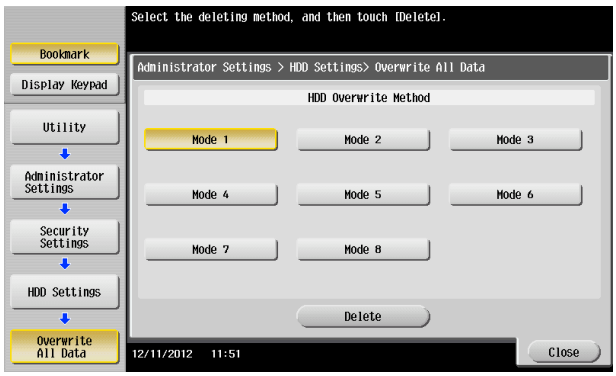
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the HDD Settings screen on the display from the control panel.

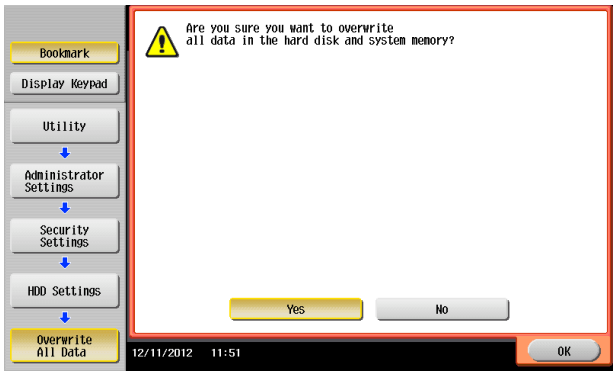
2 Touch [Overwrite All Data].



3 Select the desired mode and touch [Delete].



4 A confirmation message appears. Select [Yes] and touch [OK].



5 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.

➔ Check that all data has been overwritten and erased properly. Data is not erased properly if an error occurs during the procedure. For details, contact your Service Representative.

➔ When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. if there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

➔ After the main power switch has been turned on, quickly turn it off and give the machine to the Service Engineer. If the Overwrite All Data function is executed by mistake, contact the Service Engineer. For details, contact your Service Representative.

2.14 Obtaining Job Log

When access to the machine by the administrator of the machine through the Administrator Settings from the control panel is authenticated, the machine enables acquisition and deletion of a Job Log. The Job Log (Audit Log) is a function that stores information on, for example, operations performed in the machine and a job history in the HDD. Setting the Job Log (Audit Log) allows an illegal act or inadequate operation performed on the machine to be traced.
The obtained Job Log can be downloaded and viewed from the PageScope Web Connection.

NOTICE
Job Log obtains time/date information. So, set an accurate time/date in the machine in advance. For more details on the time/date setting, see page 2-79.

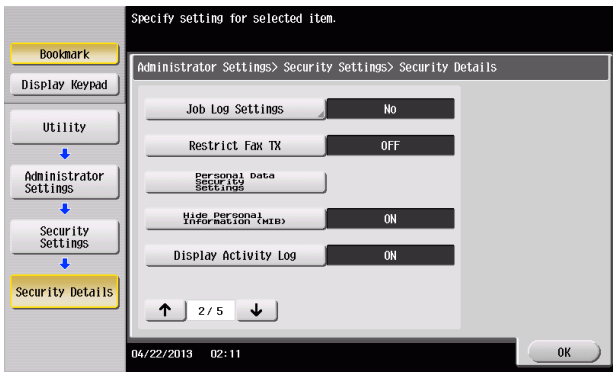
Log Type	Description	
[Accounting Log]	Enables you to obtain information relevant to paper consumption for each user or account.	
[Counting Log]	Enables you to obtain information about paper consumption and the reduction rate of paper used for printing.	
[Audit Log]	Enables you to obtain user operation or job history. Audit Log is concerned mainly with the following events. It is recommended that Audit Log be backed up at regular intervals. The machine is capable of saving up to about 20,000 records of Audit Log. The maximum number of days the records can be saved depends on the operating condition of the machine. For example, identify the output volume of the audit log by operating the machine for several days and estimate adequate frequency of the backup operation.	
	Log relating to jobs	• Jobs stored in boxes in the copy, scan, or box mode from the control panel • Jobs stored in boxes via the printer driver, and print jobs • Jobs stored in boxes from USB • Jobs stored in boxes after fax reception • Jobs output from boxes
	Log relating to authentication	• Administrator Settings • Successful or failed administrator authentication (including SNMP administrator authentication) • Successful or failed user/account authentication • Successful or failed Public User Box authentication • Successful or failed authentication of access to a Secure Print document
	Turning ON/OFF the main power switch (including starting of the Audit Log function)	

2.14.1 Obtaining and deleting a Job Log

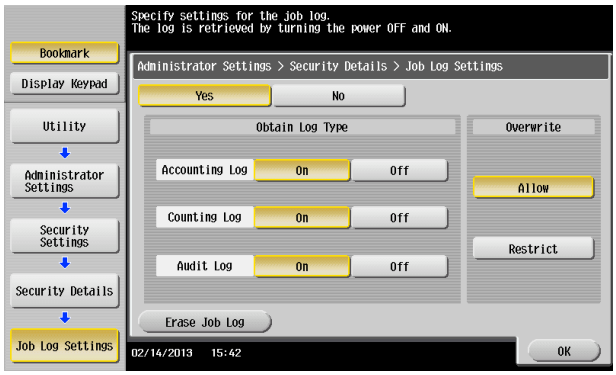
✔ For the procedure to call the Security Details screen on the display, see steps 1 and 2 of page 2-16.
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Security Details screen on the display from the control panel.

2 Touch [↓] and touch [Job Log Settings].



3 Select [Yes] and touch [On] of the specific type of log to be obtained.



➔ Under [Overwrite], whether to enable writing over old Job Logs when the Job Log space in the HDD is full of old Job Logs can be selected.

Item	Description
[Allow]	Allows Job Logs to be continuously stored by writing over old Job Logs in chronological order even when the Job Log space in the HDD is full.
[Restrict]	Displays, when the Job Log space in the HDD is full, an alarm indicating that no more Job Logs can be stored and stops storing Job Logs. After this event, no more jobs will be accepted.

➔ If [Allow] is set for [Overwrite], illegal operations performed from an external environment (such as repeated log-on procedures performed over the network) make the Job Log space full of data within a short period of time, so that older Job Log data is deleted. To avoid such a situation, the administrator of the machine should download the Job Log data at regular intervals or select [Restrict] for [Overwrite]. For details of downloading of the Job Log data, see page 2-70.

➔ If [Restrict] is selected for [Overwrite], the administrator of the machine should download Job Log data at regular intervals to thereby delete Job Logs from the machine and to ensure that the Job Log space in the HDD is not full. For details of downloading of the Job Log data, see page 2-70.

➔ If the setting for [Overwrite] is switched from [Restrict] to [Allow] after saving of Job Logs is started, overwriting is enabled with the Job Logs saved so far left as they are.

➔ If the setting for [Overwrite] is switched from [Allow] to [Restrict] after saving of Job Logs is started, overwriting is prohibited with all previously saved Job Logs deleted.

➔ Touching [Erase Job Log] erases all Job Logs saved in the machine.

4 Click [OK].
When the machine is restarted, it starts obtaining Job Logs.

2.14.2 Downloading the Job Log data

✔ For the procedure to access the Admin Mode, see page 2-2.

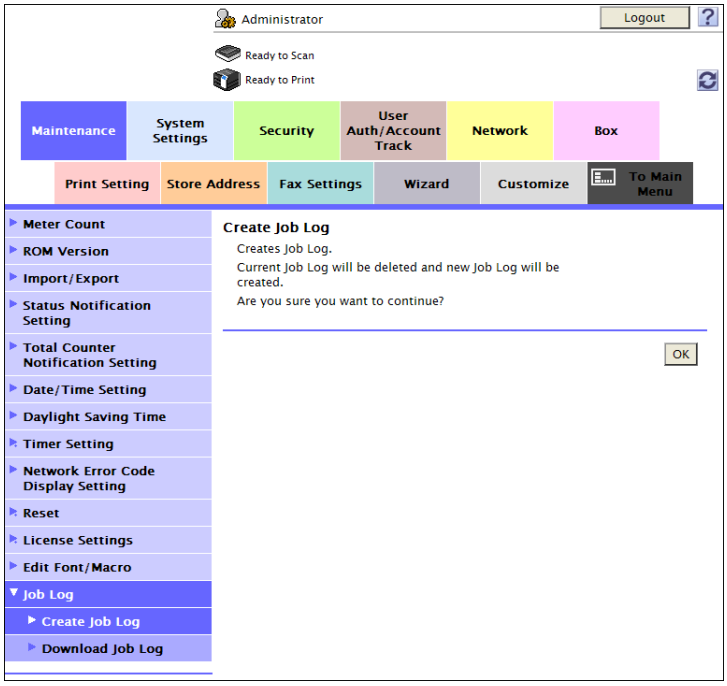
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Maintenance] tab.

3 Click [Job Log] ▸▸ [Create Job Log] from the menu.

4 Click [OK]. This starts creating job log data.



➔ If no Job Logs are saved in the machine, the machine displays an error message indicating that no Job Log data to be created is available.

➔ When the Job Log data is successfully created, the Job Log in the machine is deleted.

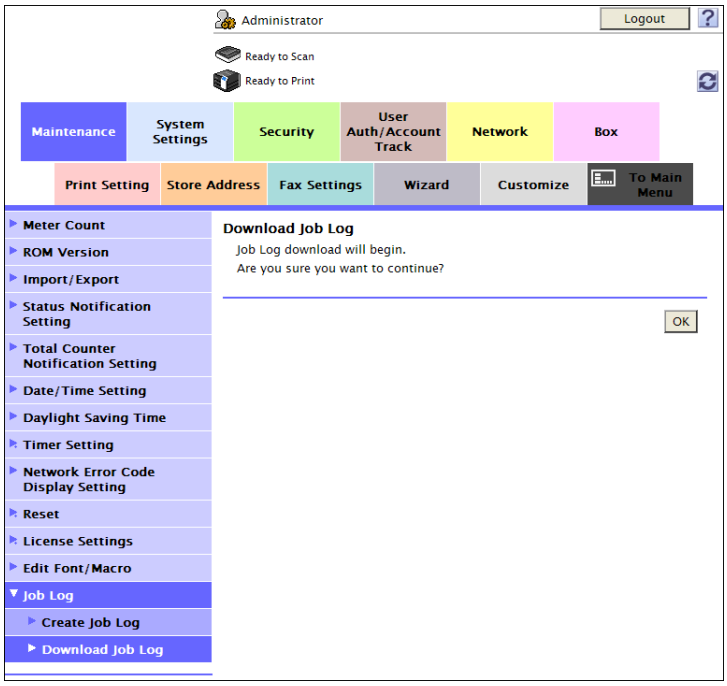
➔ The sequence of creating the Job Log data continues even when the browser is closed during the creating sequence. Restart the PageScope Web Connection and check that the Job Log data has been created.

➔ If any job logs have not been obtained, download them before creating new job log data. The job logs that have not been obtained are deleted when the new job log data is created.

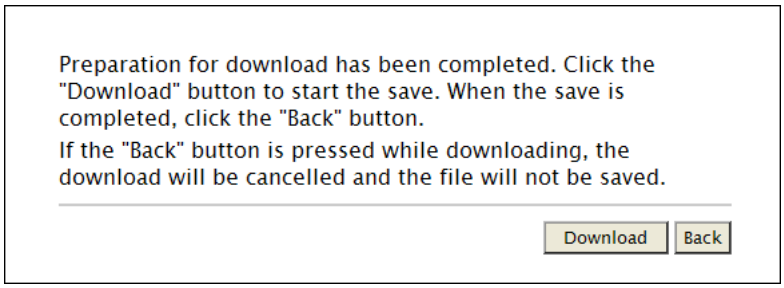
5 Click [OK].

6 Click [Job Log] ▸▸ [Download Job Log] from the menu.

7 Click [OK].



8 Click [Download].
This starts downloading the job log data.


Preparation for download has been completed. Click the "Download" button to start the save. When the save is completed, click the "Back" button.
If the "Back" button is pressed while downloading, the download will be cancelled and the file will not be saved.
Download
Back

➔ If a message appears indicating that a Job Log data file size is too large to be output, try to create the Job Log data yet to be obtained after downloading is completed.

➔ Only the administrator of the machine may handle the Job Log data that has been downloaded.

➔ The administrator of the machine should download the Job Log data at regular intervals to thereby ensure that the machine is properly used.

Job Log data

The Job Log data is read in an XML format file. The file allows various types of information to be determined, including the time/date information of log collection, information on user operations, job types, and job results.

The Job Log data represents chronological records of both "log relating to jobs" and "log relating to operations."

<Log relating to jobs>

Tag name	Tag description	Typical display	Description
ColTim	Log collection time/date	2012/4/1 12:34	Time-of-day and date when the log is collected. Time/date information of the machine is used.
LogID	Log ID	0000000001	ID number assigned to the log.
JobNam	Job name	User X	The name of the job. If a user name is known, the user name is shown.
JobTyp	Job type	1	Denotes the type of the job. [1]: Copy [2]: Print [3]: Scan [4]: Fax [5]: Fax/scan broadcast and others
JobEntTim	Job registration time/date	2012/4/1 12:34	Time/date when the job is registered.
JobFinTim	Job finish time/date	2012/4/1 12:34	Time/date when the job is finished.
OpeInf	Operator information	-	Operator who registers the job. The operator information is displayed when user operation is involved.
OpeCode	Operator code	268435457	Coded operator information. [0]: Unknown user [16777216]: Service engineer [33554432]: Administrator [83886080]: System (machine) [268435456+X]: User (X denotes a number assigned to the user) and others
OpeNam	Operator name	User X	Name of the operator.
TrcCode	Account code	268435457	Coded account information. [0]: Unknown account [67108864]: Administrator [268435456+X]: Account (X denotes a number assigned to the account) and others
TrcNam	Account name	Account X	Name of the account.

Tag name	Tag description	Typical display	Description
IFNo	Interface name	16	Denotes the interface with which the job is performed [16]: Control panel [32]: Printer reception [64]: Fax reception [80]: System [96]: PageScope Web Connection [112]: TCP Socket [128]: OpenAPI * [144]: SNMP (MIB) and others * May be recorded as OpenAPI even when the PageScope Web Connection is used.
JobResInf	Job result	-	Result of the job.
JobRes	Job result	0	Denotes the result of the job. [0]: Normally terminated [513]: Deleted by user and others
ScProc	Scan process	-	Scan process information.
ActStTim	Scan start time/date	2012/4/1 12:34	Time/date when the scan operation is started.
ActFinTim	Scan finish time/date	2012/4/1 12:34	Time/date when the scan operation is finished.
Res	Scan process result	0	Result of the scan process. [0]: Normally terminated [65535]: Abnormally terminated
PrtProc	Print process	-	Print process information.
Res	Print process result	0	Result of the print process. [0]: Normally terminated [65535]: Abnormally terminated
ProcNetTX	Network transmission process	-	Network transmission process information.
Protcol	Protocol/ address type	7	Denotes the protocol/address type used for transmission. The PageScope Web Connection protocol is HTTP. [7]: HTTP [225]: External memory [241]: Box and others
Port	Port number	50001	Denotes the port number used during transmission.
DstInf	Destination information	XXX.XXX.XXX.XXX	Denotes information on the destination.
FileNam	File name	SCXXX.pdf	Denotes the name of the transmission file.
Res	Network transmission process result	0	Result of the network transmission process. [0]: Normally terminated [65535]: Abnormally terminated
NetFaxProcTX	Network fax transmission process	-	Information on the network fax transmission process.
Res	Network fax transmission process result	0	Result of the network fax transmission process. [0]: Normally terminated [65535]: Abnormally terminated

Tag name	Tag description	Typical display	Description
NetFaxProcRX	Network fax reception process	-	Information on the network fax reception process.
Res	Network fax reception process result	0	Result of the network fax reception process. [0]:Normally terminated [65535]:Abnormally terminated
FaxProcTX	Fax transmission process	-	Information on the fax transmission process.
ActTimTX	Time/date of transmission	2012/4/1 12:34	Denotes the time/date of transmission.
DstInfTX	Destination information	00-0000-0000	Denotes information on the destination.
Res	Fax transmission process result	0	Result of the fax transmission process. [0]: Normally terminated [65535]: Abnormally terminated
FaxProcRX	Fax reception process	-	Information on the fax reception process.
ActTimRX	Time/date of reception	2012/4/1 12:34	Denotes the time/date of reception.
DstInfRX	Transmitter information	00-0000-0000	Denotes information on the transmitter.
Res	Fax reception process result	0	Result of the fax reception process. [0]: Normally terminated [65535]: Abnormally terminated
BxRdProc	Retrieve from box process	-	Information on the process of retrieving from box.
BoxNo	Box number	XXXXXXXXXX	Denotes the number assigned to the box from which the document is to be retrieved. [0]: Memory RX Box [1000020130]: Password Encrypted PDF Box [1000020150]: ID & Print box [1000030040]: Secure Print box [1 to 999999999]: Displays the box number if it has been registered, such as with a Public User Box or an Annotation Box. and others
DcNam	Document name	XXXXX	Denotes the name of the document to be retrieved from the box.
Res	Retrieve from box process result	0	Result of the process of retrieving from box. [0]: Normally terminated [65535]: Abnormally terminated
BxWtProc	Save to box process	-	Information on the process of saving data in box.
WtBxNo	Box number	XXXXXXXXXX	Denotes the number assigned to the box in which the document is to be stored. [0]: Memory RX Box [1000020130]: Password Encrypted PDF Box [1000020150]: ID & Print box [1000030040]: Secure Print box [1 to 999999999]: Displays the box number if it has been registered, such as with a Public User Box or an Annotation Box. and others
WtDcNam	Document name	XXXXX	Denotes the name of the document to be stored in the box.

Tag name	Tag description	Typical display	Description
Res	Save to box process result	0	Result of the process of saving data in the box. [0]: Normally terminated [65535]: Abnormally terminated
PrtProcRX	Network reception process	-	Information on the network reception process.
Res	Network reception process result	0	Result of the network reception process. [0]: Normally terminated [65535]: Abnormally terminated
ExtOutProc	External output process	-	Information on the external output process.
Res	External output process result	0	Result of the external output process. [0]: Normally terminated [65535]: Abnormally terminated

<Log relating to operations>

Tag name	Tag description	Typical display	Description
Code	Operation code	1281	Denotes the specific operation performed. [1]: Turning ON or OFF the log function [2]: Log overflow [3]: Deleting log [4]: Missing log detected * [257]: Service mode authentication (logon) [258]: Service mode authentication (logoff) [513]: Administrator setting authentication (logon) [514]: Administrator setting authentication (logoff) [516]: Canceling the lock state when the administrator setting authentication fails [517]: Changing the administrator password in the administrator setting [785]: Changing the authentication mode setting in the administrator setting [804]: Canceling the lock state when the user/account authentication fails in the administrator setting [805]: Registering a user in the administrator setting [806]: Deleting a user in the administrator setting [807]: Changing a user password in the administrator setting [809]: Changing a user attribute in the administrator setting [811]: Registering a user (automatic registration) [812]: Setting/changing the account to which a user belongs in the administrator setting [813]: Temporarily suspending or resuming use by a user in the administrator setting [821]: Registering an account in the administrator setting [822]: Deleting an account in the administrator setting [823]: Changing an account password in the administrator setting [825]: Changing an account attribute in the administrator setting [827]: Changing an account name in the administrator setting [828]: Temporarily suspending or resuming use by an account in the administrator setting [837]: Registering a box in the administrator setting [838]: Deleting a box in the administrator setting [839]: Changing a box password in the administrator setting [841]: Changing a box attribute in the administrator setting [856]: Changing ID & Print setting in the administrator setting [865]: Changing the "user change permission" setting in address settings in the administrator setting [869]: Preparing, changing, or deleting address data in the administrator setting [875]: Registering, changing, or deleting an S/MIME certificate in the administrator setting

Tag name	Tag description	Typical display	Description
Code	Operation code	1281	[1025]: Enhanced security setting in the administrator setting [1026]: Changing the password rule setting in the administrator setting [1028]: Changing an operation prohibited function when the authentication fails in the administrator setting [1031]: Changing the Overwrite HDD Data setting in the administrator setting [1034]: Network setting change in the administrator setting [1035]: Changing the HDD encryption setting in the administrator setting [1036]:Changing the HDD encryption word in the administrator setting [1038]: Changing the release time settings in the administrator setting [1039]:Changing the check count for Prohibited Functions When Authentication Error in the administrator setting [1281]: User authentication (logon) [1282]: User authentication (logoff) [1287]: Changing the user password by a user [1291]: Setting or changing the account to which a particular user belongs by the user [1297]: Account authentication (logon) [1298]: Account authentication (logoff) [1313]: Authentication by SNMPv3 write authority in the administrator setting (password matching only) [1322]: Changing the WebDAV server password in the administrator setting [1537]: Box authentication by user (ID/password matching only) [1541]: Box registration by user [1558]: Deleting document from box by user [1563]: Moving documents across boxes by user [1564]: Copying documents in box by user [1569]: Authentication of access to Secure Print document by user (ID/password matching only) [1574]: Deleting Secure Print document by user [1825]: Backup, export [1826]: Restore, import [2561]: Turning main power switch ON [2577]: Turning main power switch OFF [3073]: Changing time/date in the administrator setting (manual setting) [3075]: Changing the system auto reset time in the administrator setting [3329]: Changing the S/MIME setting in the administrator setting [3331]: Changing the SNMPv3 Write Auth/Priv password in the administrator setting [3333]: Changing the SSL/TLS strength setting in the administrator setting [3585]: Changing the TSI reception setting in the administrator setting and others * Displayed if there is a logon event but not a logoff event, such as when the machine develops a fault after a user logged on, so that the user was unable to log off.
Tim	Time/date of operation	2012/4/1 12:34	Denotes time/date when the operation is performed.

Tag name	Tag description	Typical display	Description
ResCode	Result code	0	Denotes the result of operation. [0]: Normally terminated [257]: Authentication failed and others
OperatCont	Details of operation	1	Denotes the specific detail of operation. [1]: Enable [2]: Disable and others
BoxOperat	Box operation information	-	Denotes information on box operation.
TrgBoxNo	Box number to be operated	XXXXXXXXXX	Denotes the box number relative to box operations or document operations in a box. [0]: Memory RX Box [1000020130]: Password Encrypted PDF Box [1000020150]: ID & Print box [1000030040]: Secure Print box [1 to 999999999]: Displays the box number if it has been registered, such as with a Public User Box or an Annotation Box. and others
MovBoxNo	Move destination box number	XXXXXXXXXX	Denotes the number assigned to the box to which the document in question is to be moved.
CpyBoxNo	Copy destination box number	XXXXXXXXXX	Denotes the number assigned to the box to which the document in question is to be copied.
SecretID	Secure Print ID	XXXXX	Denotes the ID used for accessing a Secure Print document

2.15 Setting time/date in machine

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the time-of-day and date. Use of the network time protocol (NTP) server allows the current time/date to be adjusted automatically.

NOTICE

If the NTP server is to be used, make sure that the NTP server is a correct one and take necessary action to protect communications between the NTP server and the machine.

2.15.1 Setting time/date

<From the Control Panel>

✔ For the procedure to call the System Settings screen on the display, see steps 1 and 2 of page 2-28.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the System Settings screen on the display from the control panel.

2 Touch [Date/Time Settings]

3 Select the item to be set. Then, touch [C] and next set the time-of-day and date.
Touching [Set Date] lets the NTP server to adjust the current time/date automatically.

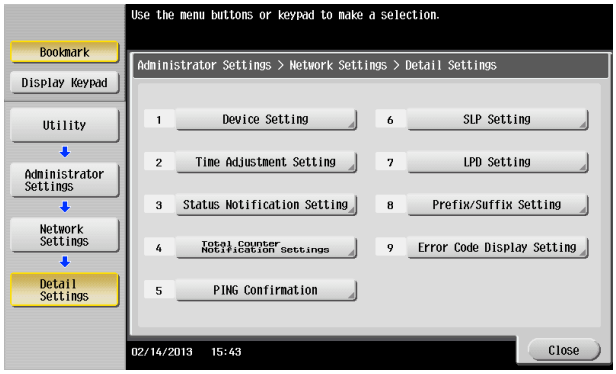
➔ Touch [Display Keypad] to display the keypad.

➔ If [Set Date] is to be used for the setting, set the time difference from the coordinated universal time (UTC) using [Time Zone].

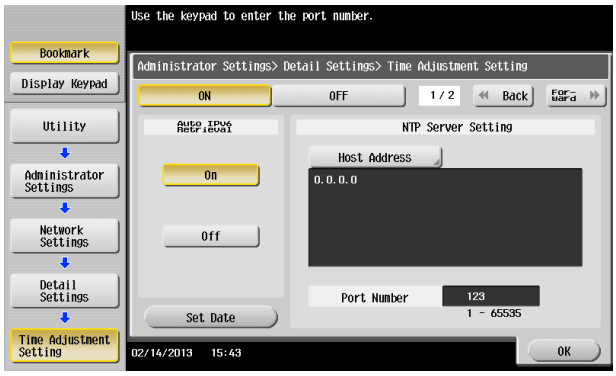
➔ [Set Date] can be used if the NTP server is registered. For more details, make settings of step 5 and onward.

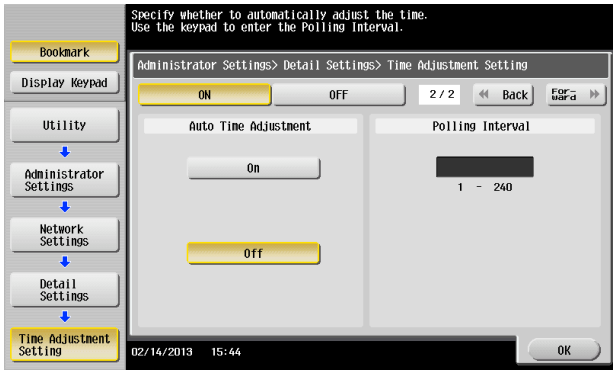
4 Touch [OK].

5 Touch [Administrator Settings] ▸▸ [Network Settings] ▸▸ [Forward] ▸▸ [Detail Settings] ▸▸ [Time Adjustment Setting].



6 Select [ON], and make the necessary settings.





➔ If [Auto Time Adjustment] is set to [On], the machine connects to the NTP server at regular intervals to thereby adjust the time-of-day and date. In this case, use [Polling Interval] to set the interval at which the time/date adjustment is to be made (unit: hours).

7 Touch [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

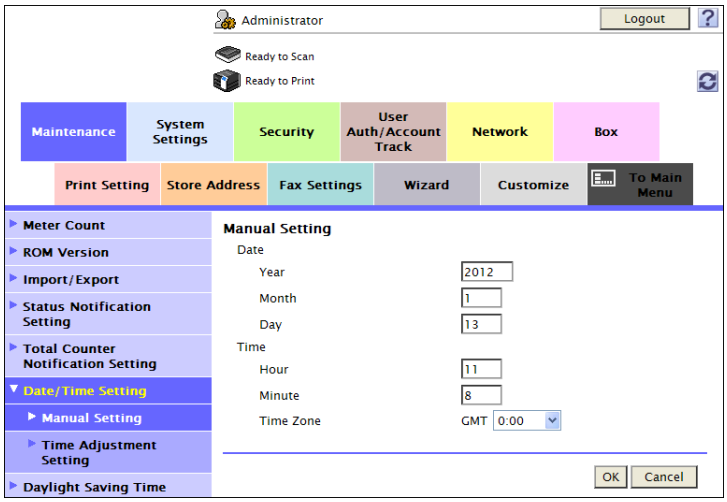
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Maintenance] tab.

3 Click [Date/Time Setting] ▸▸ [Manual Setting] from the menu.

4 Enter the time-of-day and date and click [OK].



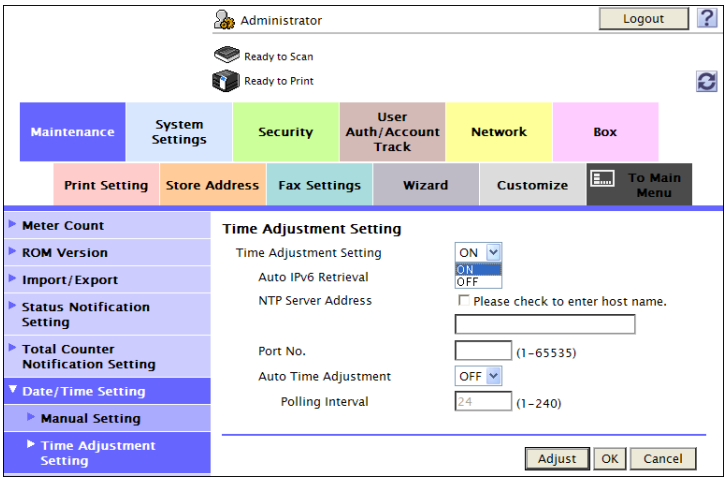
➔ To correct the time-of-day, use [Time Zone] to set the time difference from the coordinated universal time (UTC).

5 Check that a message indicating that the setting is completed appears. Then, click [OK].

➔ To correct the time-of-day using the NTP server, make the following settings.

6 Click [Date/Time Setting] ▸▸ [Time Adjustment Setting] from the menu.

7 Click [ON] from the pull-down menu of [Time Adjustment Setting], and make the necessary settings.



➔ If [Auto Time Adjustment] is set to [ON], the machine connects to the NTP server at regular intervals to thereby adjust the time-of-day and date. In this case, use [Polling Interval] to set the interval at which the time/date adjustment is to be made (unit: hours).

8 Click [Adjust].

9 Check that a message indicating that the adjustment is completed appears. Then, click [OK].

2.15.2 Setting daylight saving time

<From the Control Panel>

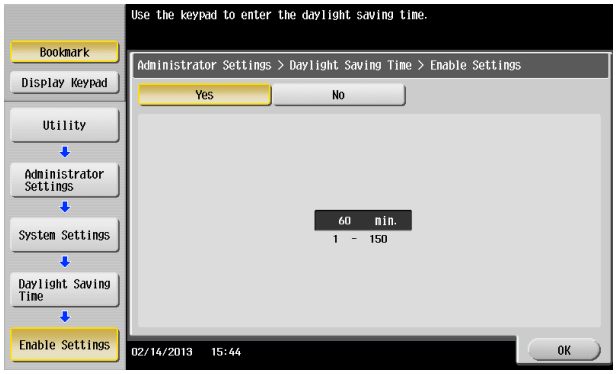
✔ For the procedure to call the System Settings screen on the display, see steps 1 and 2 of page 2-28.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the System Settings screen on the display from the control panel.

2 Touch [Daylight Saving Time] ▸▸ [Enable Settings].

3 Select [Yes]. Then, touch [C] and enter time to be advanced as the daylight saving time.



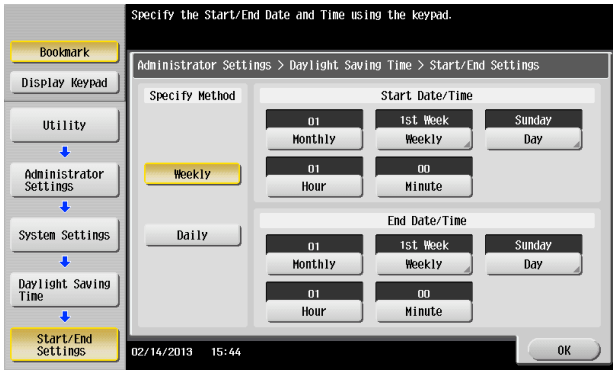
➔ Touch [Display Keypad] to display the keypad.

➔ The current time is set forward to reflect daylight saving time.

4 Touch [OK].

5 Touch [Start/End Settings].

6 Select [Weekly] or [Daily]. Then, specify the start date/time and the end date/time of a period of time to which the daylight saving time is applicable.



7 Touch [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

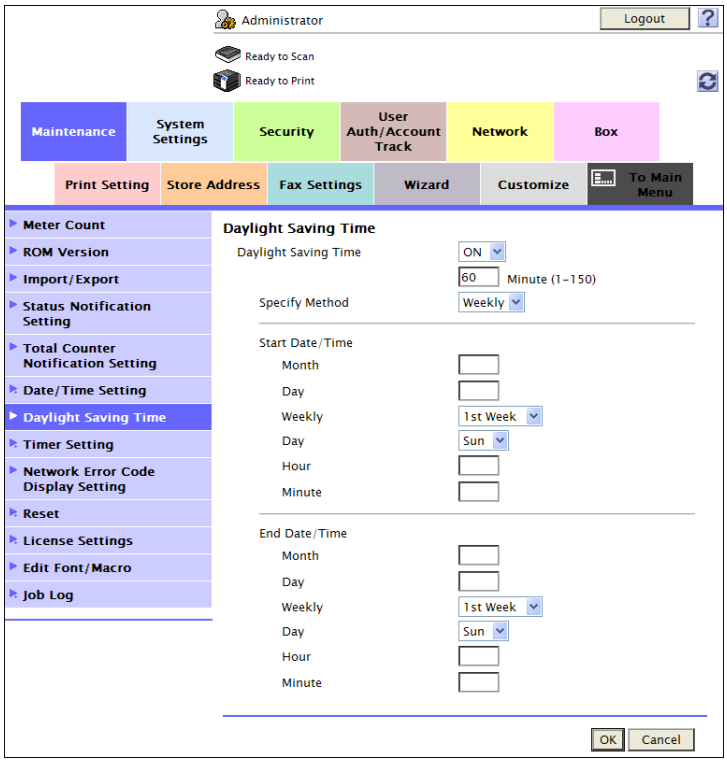
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Maintenance] tab.

3 Click [Daylight Saving Time] from the menu.

4 Select [ON] from the pull-down menu of [Daylight Saving Time], and enter time to be advanced as the daylight saving time.
From the [Specify Method] pull-down menu, select [Weekly] or [Daily] and specify the start date/time and the end date/time of a period of time to which the daylight saving time is applicable.



5 Click [OK].

6 Check that a message indicating that the adjustment is completed appears. Then, click [OK].

2.16 SSL Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables the setting of encryption of image data transmitted and received between the PC and the machine.

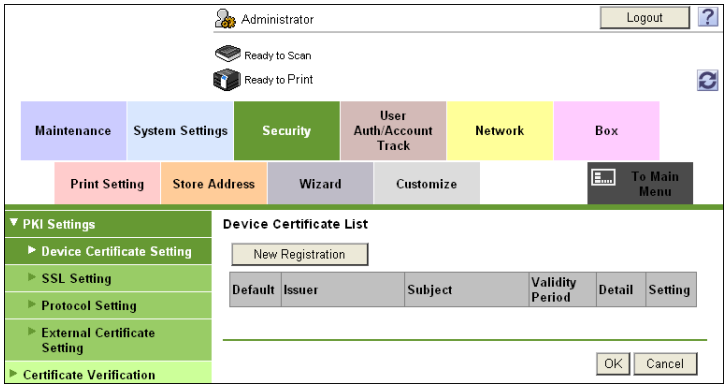
2.16.1 Device Certificate Setting

- ✔ For the procedure to access the Admin Mode, see page 2-2.
- ✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.
- ✔ The key length set for the public key of the server generated in SSL certificate setting is 1024 bits.

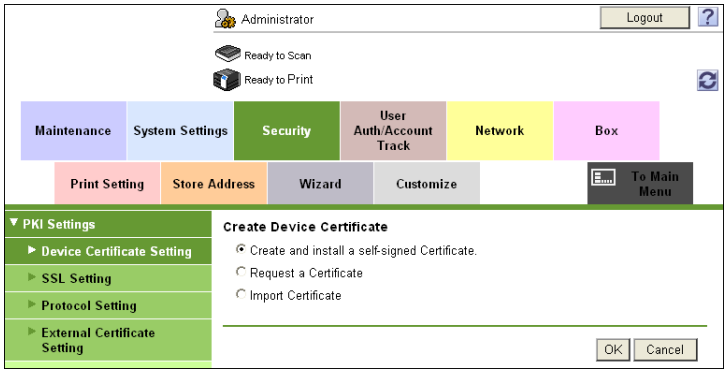
1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Security] tab.

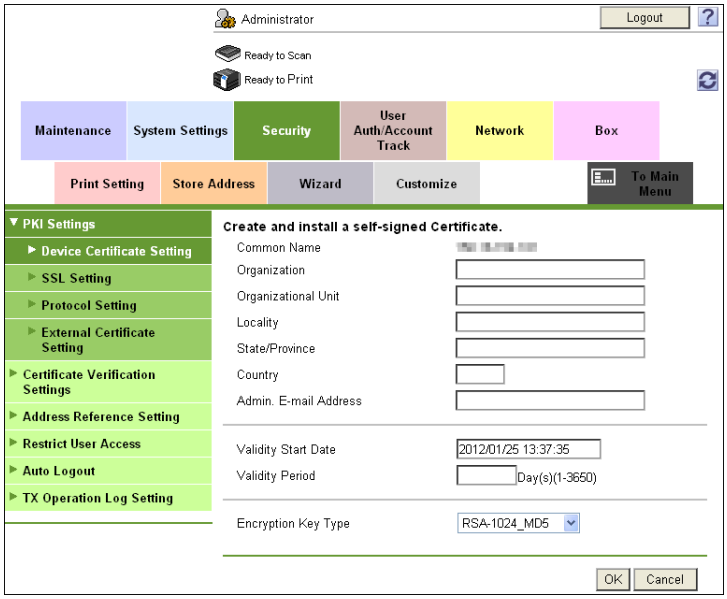
3 Click [New Registration].



4 Select [Create and install a self-signed Certificate] and click [OK].



5 Make the necessary settings.



➔ If data entered for each item does not meet the requirements, a message appears that tells that the data entered is wrong.

6 Click [OK].
The certificate can now be registered.

2.16.2 SSL Setting

✔ For call the PKI Settings screen on the display, see steps 1 and 2 of page 2-84.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

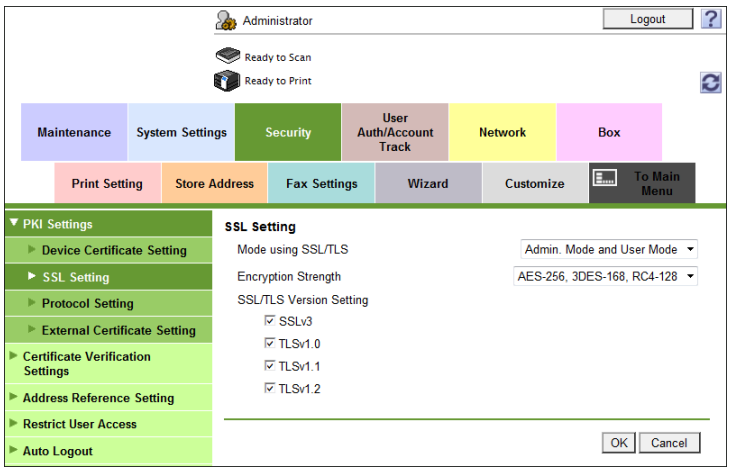
NOTICE

When making the SSL Setting, be sure to make sure in advance that the device certificate has been registered in the machine. For the procedure to register the device certificate, see page 2-84.

1 Start PageScope Web Connection and call the PKI Settings screen on the display.

2 Click [SSL Setting] from the menu.

3 Set "Mode using SSL/TLS" and "Encryption Strength" and click [OK].



➔ Select "Admin. Mode and User Mode" for "Mode using SSL/TLS."

➔ For encryption strength, select the strong "AES-256, 3DES-168."

➔ The Enhanced Security Mode is canceled, if setting containing strength lower than AES/3DES is selected when the Enhanced Security Mode is [ON].

➔ Cancel the selection of "SSLv3" of SSL/TLS Version Setting.

4 Click [OK].

2.16.3 Removing a Certificate

✔ For call the PKI Settings screen on the display, see steps 1 and 2 of page 2-84.

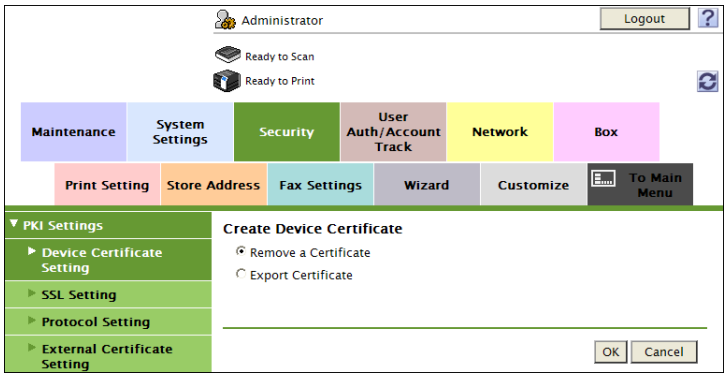
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

✔ In the Enhanced Security Mode, no certificates can be removed.

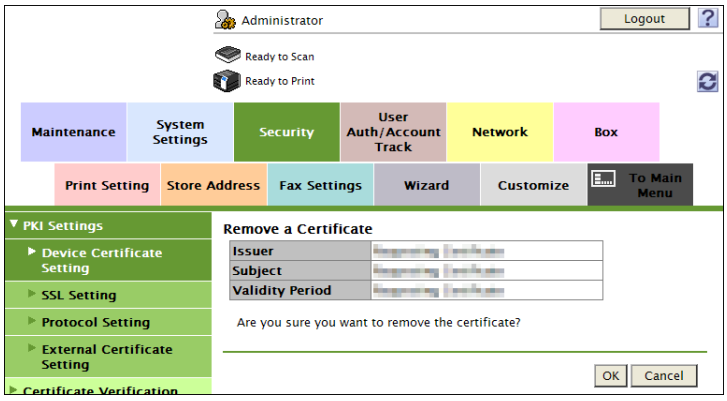
1 Start PageScope Web Connection and call the PKI Settings screen on the display.

2 Click [Setting].

3 Select [Remove a Certificate] and click [OK].



4 Click [OK].



5 Click [OK] and restart the machine.

2.17 S/MIME Communication Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables the setting of encryption of text of e-mail transmitted and received between the PC and the machine.

NOTICE

To send S/MIME communications, it becomes necessary to register the certificate at the destination. Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.

Do not use any invalid certificate, as an increased risk results of data to be protected being tampered with or leaked.

The Enhanced Security Mode is canceled, if [Automatically Obtain Certificates] is set to [Yes] when the Enhanced Security Mode is [ON].

2.17.1 Setting the S/MIME Communication

<From the Control Panel>

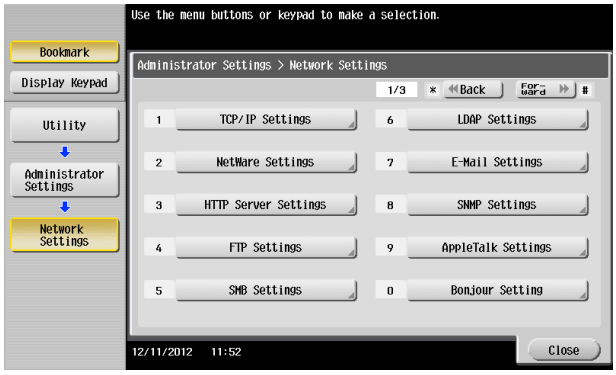
✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

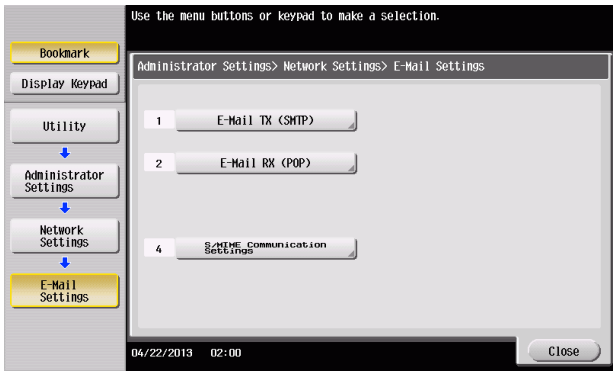
1 Call the Administrator Settings on the display from the control panel.

2 Touch [Network Settings].

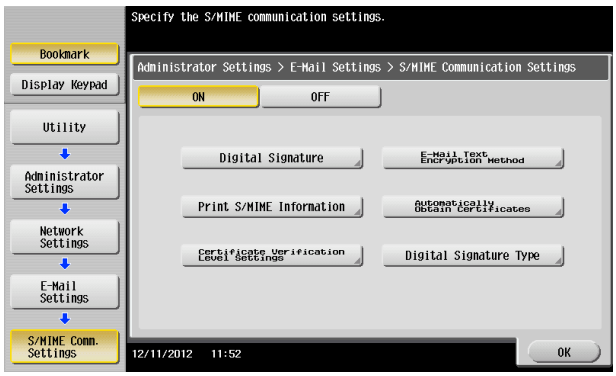
3 Touch [E-Mail Settings].



4 Touch [S/MIME Communication Settings].

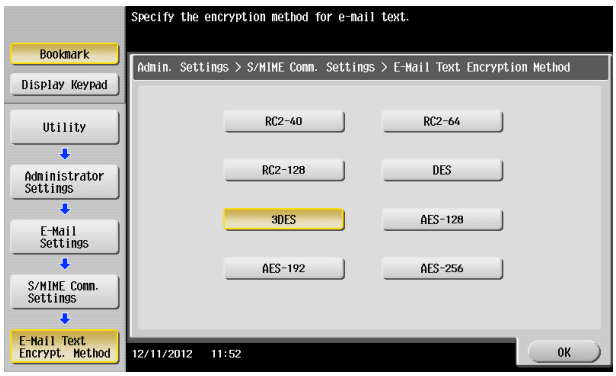


5 Select [ON] and [E-Mail Text Encryption Method].



➔ To Select [ON], the administrator's e-mail address specified in the device registration needs to correspond with the e-mail address specified at the time of certification creation.

6 Select encryption method and touch [OK].



➔ For encryption method, select the strong [3DES], [AES-128], [AES-192], or [AES-256]. If the mail software being used does not support AES, encrypted mail messages may be received, but they cannot be decrypted. Use AES-compliant mail software or select the encryption method that is the strongest of all compliant with the currently used mail software.

➔ Each encryption method represents the following.

Name	Encryption Algorithm	Encryption Key Length
[3DES]	3 key triple DES	168 bits
[AES-128]	AES	128 bits
[AES-192]	AES	192 bits
[AES-256]	AES	256 bits

➔ The Enhanced Security Mode is canceled, if the setting is changed to "RC2" or "DES" when the Enhanced Security Mode is [ON].

7 Touch [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

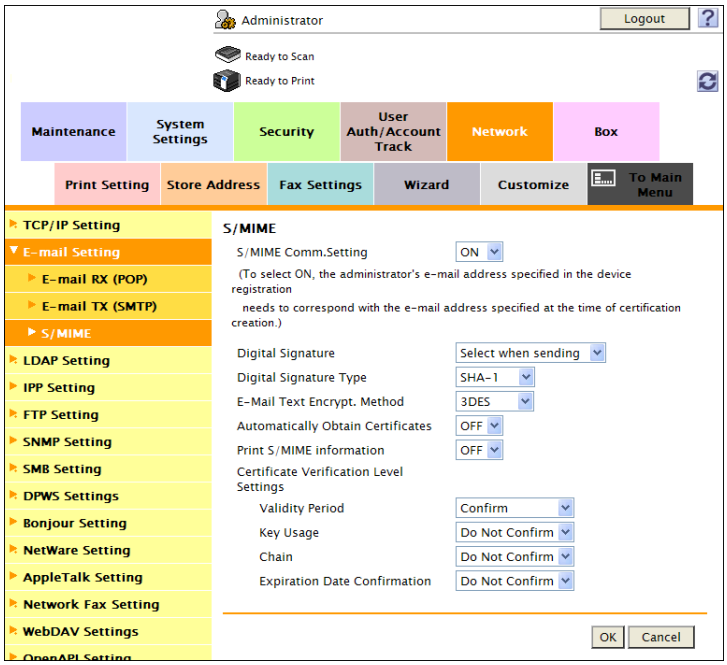
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Network] tab.

3 Click [E-mail Setting] ▸▸ [S/MIME] from the menu.

4 Make the necessary settings.



➔ For encryption method, select the strong [3DES], [AES-128], [AES-192], or [AES-256]. If the mail software being used does not support AES, encrypted mail messages may be received, but they cannot be decrypted. Use AES-compliant mail software or select the encryption method that is the strongest of all compliant with the currently used mail software.

➔ Each encryption method represents the following.

Name	Encryption Algorithm	Encryption Key Length
[3DES]	3 key triple DES	168 bits
[AES-128]	AES	128 bits
[AES-192]	AES	192 bits
[AES-256]	AES	256 bits

➔ The Enhanced Security Mode is canceled, if the setting is changed to "RC2" or "DES" when the Enhanced Security Mode is [ON].

5 Click [OK].

2.17.2 Registering the certificate

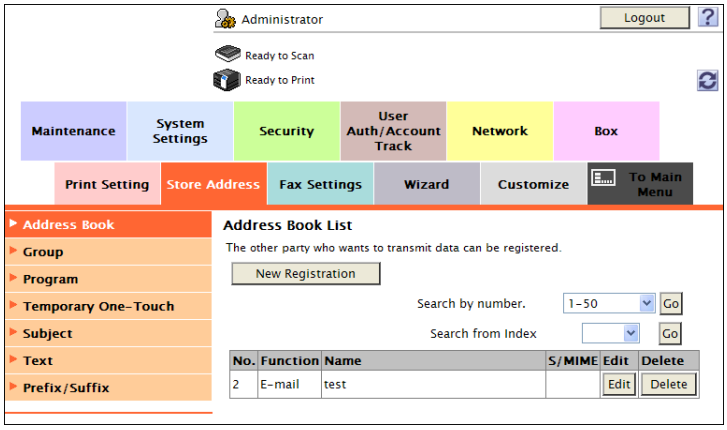
✔ For the procedure to access the Admin Mode, see page 2-2.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

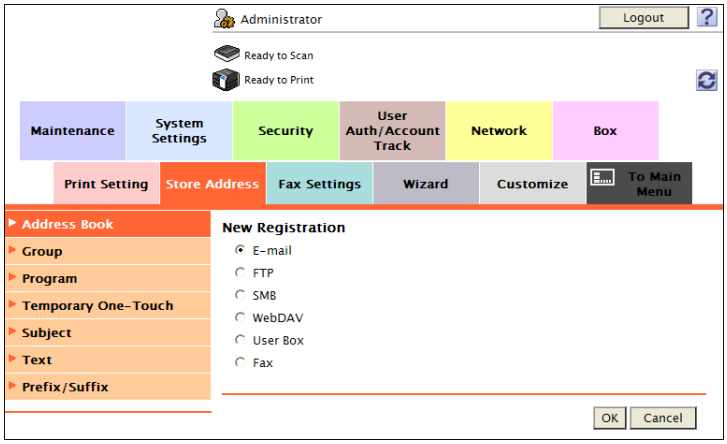
2 Click the [Store Address] tab.

3 Click [New Registration].

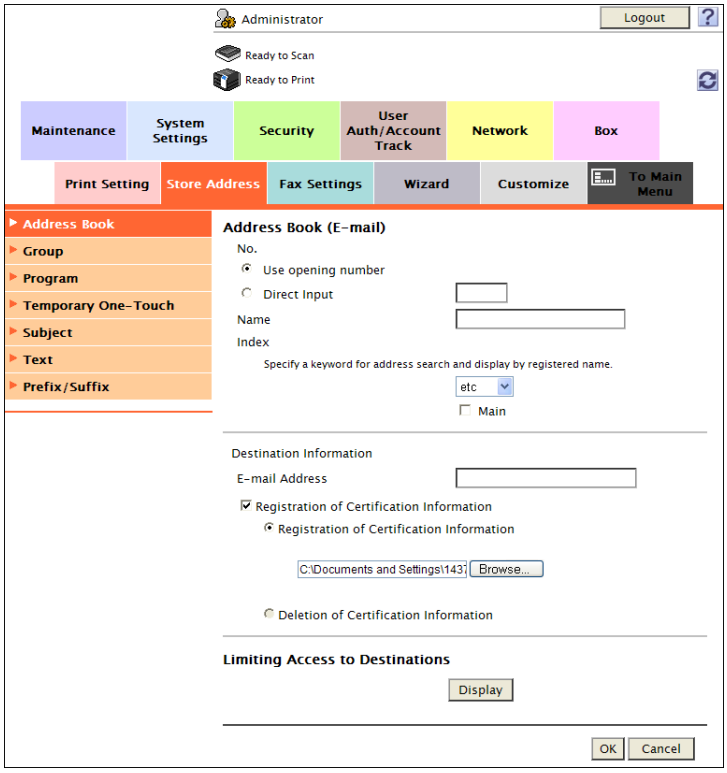


➔ To change the details of a previously registered destination, click [Edit].

4 Select [E-mail] and click [OK].



5 Click to select the [Registration of Certification Information] check box, and through [Browse], set the certificate information. If certificate information is to be deleted, select [Deletion of Certification Information].



➔ Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.

6 Make the necessary settings.

➔ A number that already exists cannot be redundantly registered.

➔ If Name and E-mail Address have not been registered, a message appears that tells that Name and E-mail Address are yet to be entered. Enter the correct Name and E-mail Address.

7 Click [OK].

2.18 SNMP Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables changing of the SNMP v3 Write User Password (auth-password, priv-password) required for accessing the MIB object over the network using the SNMP from the PC. In PageScope Web Connection, import/export of the Device Setting is enabled, allowing the setting for Security Level of SNMP v3 Setting to be saved or the saved backup data to be restored.

The auth-password and priv-password are controlled based on passwords that meet the Password Rules and the password entered is displayed as "*" or "●."

NOTICE

Operate the machine with the SNMP function disabled. If it is unavoidable to use the SNMP function, make sure of utmost security during its use and be sure to disable it after use.

2.18.1 Changing the auth-password and priv-password

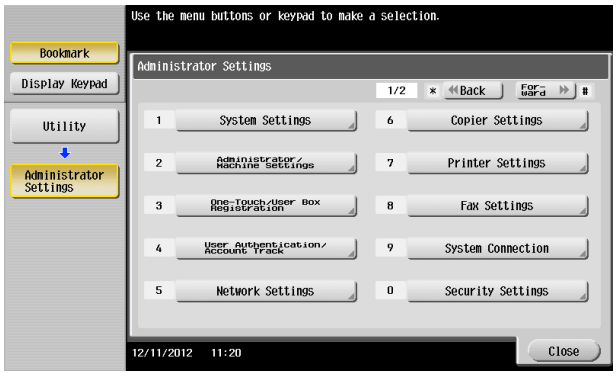
<From the Control Panel>

✔ For the procedure to call the Administrator Settings on the display, see page 2-2.

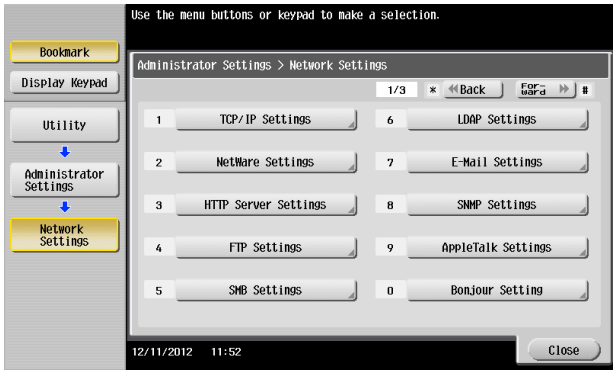
✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Administrator Settings on the display from the control panel.

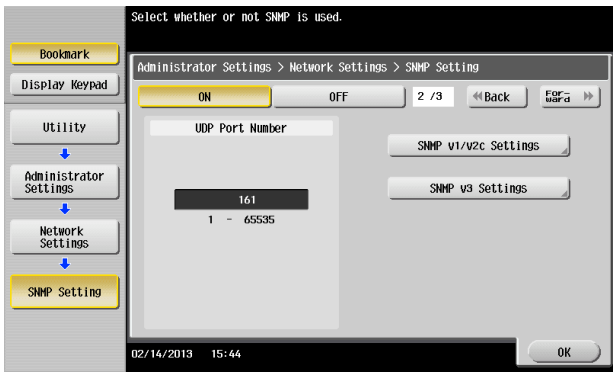
2 Touch [Network Settings].



3 Touch [SNMP Settings].

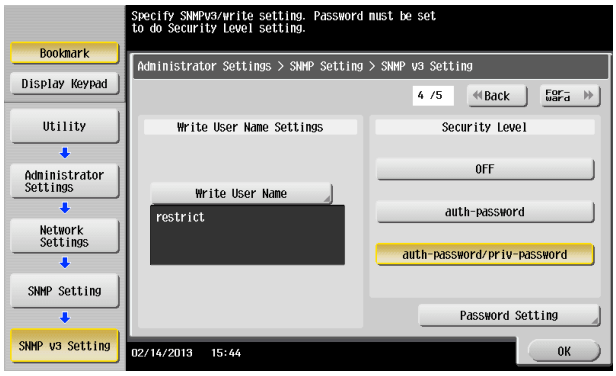


4 Touch [Forward] and, on screen "2/3", touch [SNMP v3 Settings].



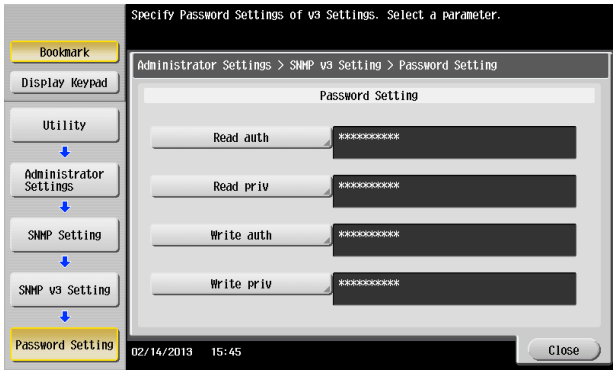
5 Touch [Forward] and call screen "4/5" of SNMPv3/Write Settings.

6 Select [auth-password] or [auth-password/priv-password] of Security Level and touch [Password Setting].



➔ The Enhanced Security Mode is canceled, if [Security Level] is set to [OFF] when the Enhanced Security Mode is [ON].

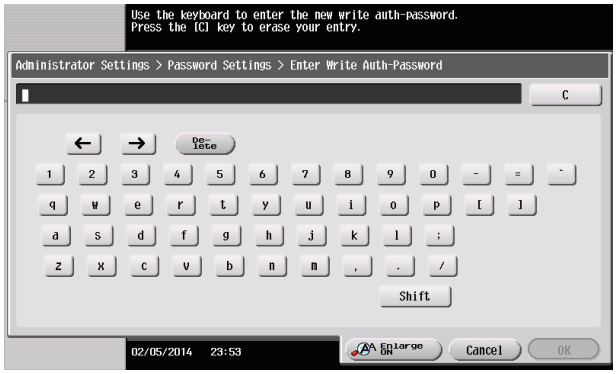
7 Touch [Write auth].



➔ When a screen appears that prompts you to enter the current password, enter the MAC Address that is set in the machine. To check the MAC Address, from [Network Settings] of step 2, select [Forward] ▸▸ [Detail Settings] ▸▸ [Device Setting].

➔ The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, perform the Release Setting by the administrator of the machine.

8 Enter the new auth-password from the keyboard.



➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

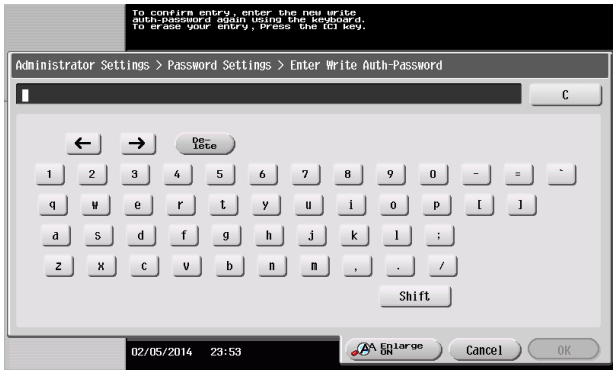
➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the previous screen.

9 Touch [OK].

➔ If the entered auth-password does not meet the Password Rules, a message that tells that the entered auth-password cannot be used appears. Enter the correct auth-password. For details of the Password Rules, see page 1-11.

10 To prevent entry of a wrong password, enter the auth-password again.



➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.

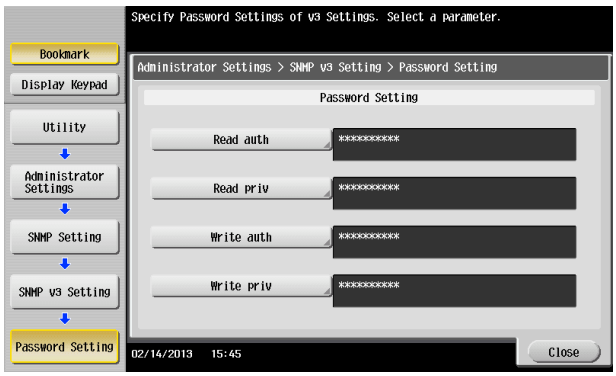
➔ Touch [Cancel] to go back to the previous screen.

11 Touch [OK].

➔ Go to step 12 if [auth-password/priv-password] is selected in step 6.

➔ If the entered auth-password does not match, a message that tells that the auth-password does not match appears. Enter the correct auth-password.

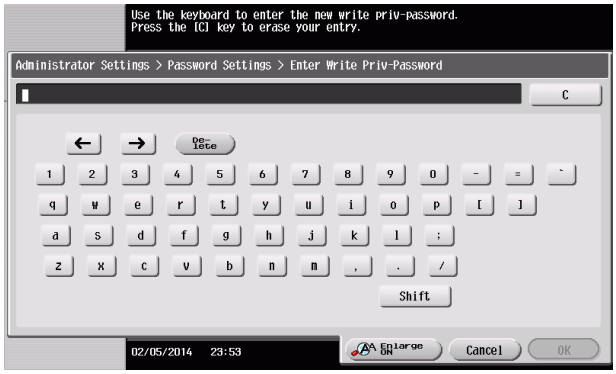
12 Touch [Write priv].



➔ When a screen appears that prompts you to enter the current password, enter the MAC Address that is set in the machine. To check the MAC Address, from [Network Settings] of step 2, select [Forward] ▸▸ [Detail Settings] ▸▸ [Device Setting].

➔ The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, perform the Release Setting by the administrator of the machine.

13 Enter the new priv-password from the keyboard.



➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

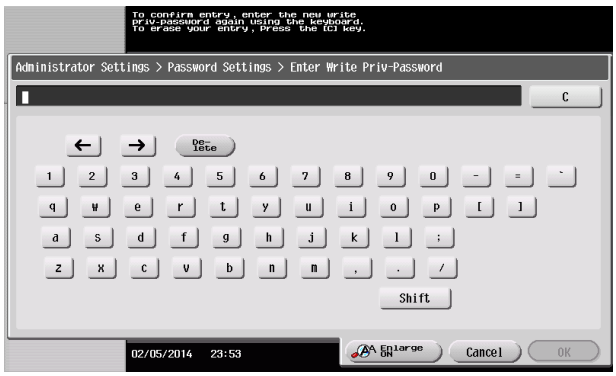
➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the previous screen.

14 Touch [OK].

➔ If the entered priv-password does not meet the Password Rules, a message that tells that the entered priv-password cannot be used appears. Enter the correct priv-password. For details of the Password Rules, see page 1-11.

15 To prevent entry of a wrong password, enter the priv-password again.


To confirm entry, enter the new write priv-password again using the keyboard. To erase your entry, press the [C] key.
Administrator Settings > Password Settings > Enter Write Priv-Password
C
Delete
Shift
02/05/2014 23:53
Enlarge On
Cancel
OK

➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

16 Touch [OK].

➔ If the entered priv-password does not match, a message that tells that the priv-password does not match appears. Enter the correct priv-password.

17 Touch [Close] and [OK].

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

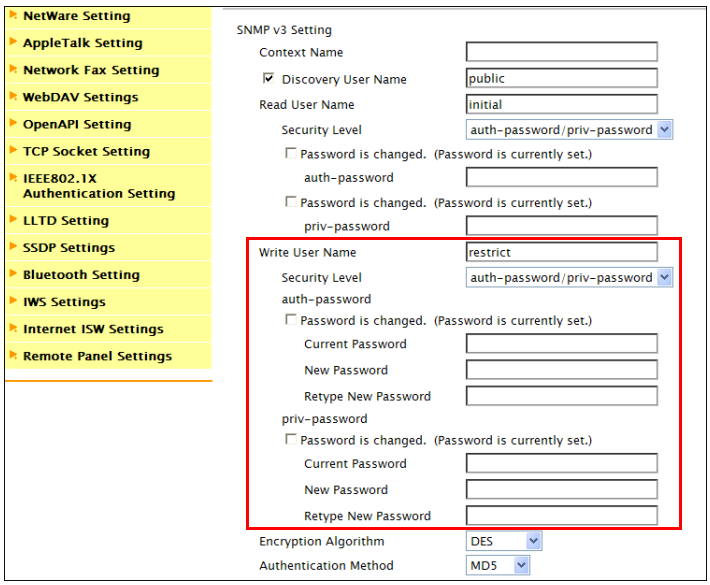
✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Network] tab.

3 Click [SNMP Setting] from the menu.

4 Enter the auth-password and priv-password in the boxes marked by the rectangle, that is, the Write side SNMP v3 Setting.



➔ For the current password, enter the MAC Address that is set in the machine. To check the MAC Address, see step 7 of page 2-93.

➔ The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, perform the Release Setting by the administrator of the machine.

5 Click [OK].

➔ If the entered auth-password or priv-password does not meet the Password Rules, a message that tells that the entered auth-password or priv-password cannot be used appears. Enter the correct auth-password or priv-password. For details of the Password Rules, see page 1-11.

➔ If the entered auth-password or priv-password does not match, a message that tells that the auth-password or priv-password does not match appears.

2.18.2 SNMP access authentication function

If the settings of the Administrator mode are to be changed using SNMP from the PC, the user attempting to gain access is authenticated to be the administrator of the machine by using the Write User Name and SNMP Password (auth-password, priv-password) of the SNMP v3 Write settings made in this machine.

Operation of the network setting function and the SNMP password change function of the security control functions that can be used over the network using SNMP is granted to the Administrator who is identified by a matching SNMP password for the Write User Name.

The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, perform the Release Setting by the administrator of the machine.

Reference

- If [auth-password] has been selected for Security Level, hashing is used for the authentication information (auth-password) to be transmitted. The machine allows you to select either HMAC-MD5 or HMAC-SHA1 for hashing.
- If [auth-password/priv-password] has been selected for Security Level, the authentication information (auth-password/priv-password) and data (object ID that specifies the object to be changed, value to be set, etc.) to be transmitted are used for hashing and encryption. Set [AES-128] for Encryption Algorithm and [SHA-1] for Authentication Algorithm.
- For accessing the MIB, use the MIB browser corresponding to the above encryption algorithm.

2.18.3 SNMP v3 setting function

The Administrator who has been authenticated through SNMP access authentication from the PC is allowed to operate the SNMP password change function.

The entry of a wrong SNMP password (auth-password, priv-password) is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong SNMP password (auth-password, priv-password) is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, perform the Release Setting by the administrator of the machine.

For the auth-password and priv-password, enter the password that meet the Password Rules. For details of the Password Rules, see page 1-11.

To change the setting, specify the corresponding object ID. See the table below for the setting items.

Setting Item	Object ID
Write User Name	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.2.2
auth-password	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.3.2
priv-password	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.4.2
Security Level	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.5.2

2.18.4 SNMP network setting function

The Administrator who has been authenticated through SNMP access authentication from the PC is allowed to operate the network setting function. To change the setting, specify the corresponding object ID. See the table below for the setting items.

Setting Item		Object ID
IP address setting	IP Address	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.3.1
	BOOT Protocol use setting	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.6.1
	BOOT Protocol Type	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.7.1
DNS server address setting		1.3.6.1.4.1.18334.1.1.2.1.5.7.1.2.1.3.1.1
SMTP server address setting		1.3.6.1.4.1.18334.1.1.2.1.5.7.13.1.1.3.1
AppleTalk Printer Name Setting		1.3.6.1.4.1.18334.1.1.2.1.5.9.2.1.3.1.1

2.19 WebDAV Function

When access to the machine by the Administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the WebDAV Server Password. The Administrator of the machine can gain access to the WebDAV Server over the network by using the WebDAV Server Password. WebDAV Server Password is controlled based on passwords that meets the Password Rules and the password entered is displayed as "*" or "●."

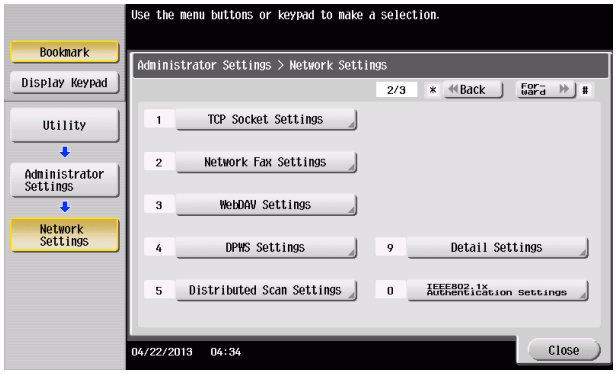
Setting the WebDAV Server Password

<From the Control Panel>

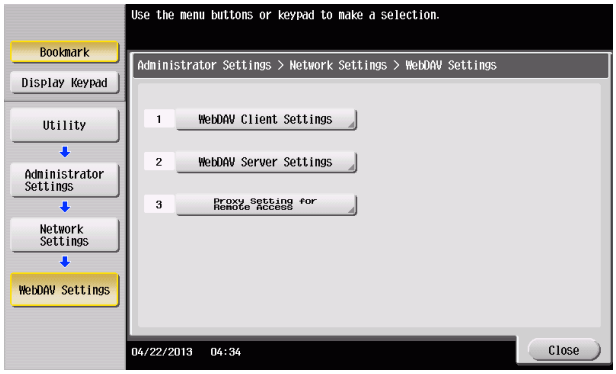
- ✔ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-93.
- ✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.
- ✔ Unauthorized access could result if the WebDAV Server Password required for accessing the WebDAV Server is incorrectly set. The Administrator of the machine should therefore make sure to set the appropriate password and control its operation so that the password is not leaked.
- ✔ The entry of a wrong WebDAV Server password is counted as unauthorized access, if the Enhanced Security Mode is set to [ON]. If a wrong WebDAV Server password is entered a predetermined number of times (twice, four times, or six times) or more set by the Administrator of the machine, the machine is set into an access lock state, rejecting any more logon attempts. To cancel the access lock state, perform the Release Setting by the Administrator of the machine.

1 Call the Network Settings screen on the display from the control panel.

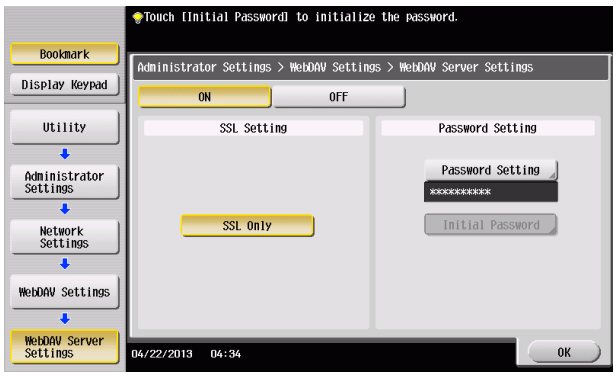
2 Touch [Forward] and touch [WebDAV Settings].



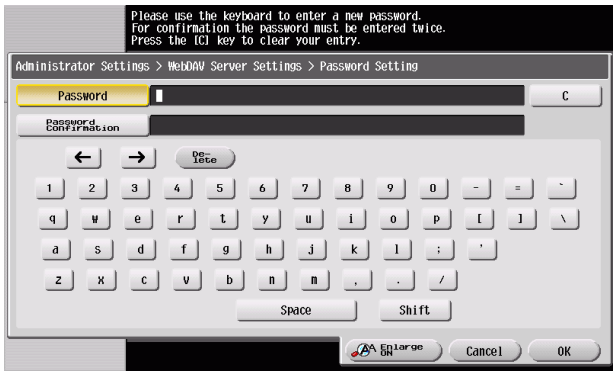
3 Touch [WebDAV Server Settings].



4 Select [ON] and touch [Password Setting].



5 Enter the new WebDAV Server Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

6 Touch [OK].

➔ If the entered WebDAV Server Password does not meet the Password Rules, a message that tells that the entered WebDAV Server Password cannot be used appears. Enter the correct WebDAV Server Password. For details of the Password Rules, see page 1-11.
➔ If the entered WebDAV Server Password does not match, a message that tells that the WebDAV Server Password does not match appears. Enter the correct WebDAV Server Password.

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

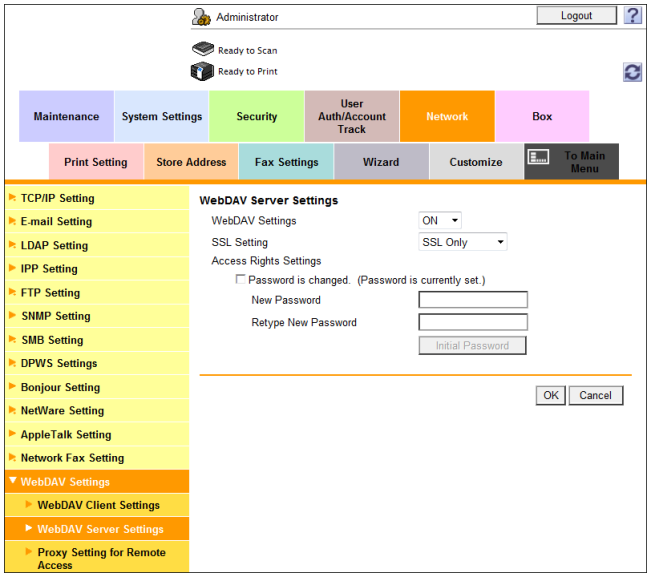
1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Network] tab.

3 Click [WebDAV Settings] ▸▸ [WebDAV Server Settings] from the menu.

4 Click the pull-down menu of WebDAV Settings and select [ON].

5 Click the [Password is changed] check box and enter the WebDAV Server Password.



6 Click [OK].

➔ If the entered WebDAV Server Password does not meet the Password Rules, a message that tells that the entered WebDAV Server Password cannot be used appears. Enter the correct WebDAV Server Password. For details of the Password Rules, see page 1-11.

➔ If the entered WebDAV Server Password does not match, a message that tells that the WebDAV Server Password does not match appears. Enter the correct WebDAV Server Password.

7 Check the message that tells that the setting has been completed. Then, click [OK].

2.20 TCP/IP Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the IP Address and registration of the DNS Server.

2.20.1 Setting the IP Address

<From the Control Panel>

✔ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-93.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Network Settings screen on the display from the control panel.

2 Touch [TCP/IP Settings].

3 Touch [IPv4 Settings].

4 Touch [Manual Input].

5 Select [IP Address] and set the IP Address.

➔ If [Auto Input] is selected for IP Application Method in step 4, select the means of acquiring the IP Address automatically from among DHCP Settings, BOOTP Settings, ARP/PING Settings, AUTO IP Settings, and the like.

6 Touch [OK].

7 Touch [OK].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Network] tab.

3 Click [TCP/IP Setting] ▸▸ [TCP/IP Setting] from the menu.

4 Select [Manual Setting] from the IP Address Setting Method pull-down menu.

5 Enter the IP Address in the "IP Address" box.

➔ If [Auto Setting] is selected from the IP Address Setting Method pull-down menu in step 4, select the means with which to acquire the IP Address automatically, including DHCP, BootP, ARP/PING, and Auto IP setting, and click the check box.

6 Click [OK].

2.20.2 Registering the DNS Server

<From the Control Panel>

✔ For the procedure to call the TCP/IP settings screen on the display, see steps 1 and 2 of page 2-103.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the TCP/IP Settings screen on the display from the control panel.

2 Make the necessary settings for the DNS Server.

➔ If [Enable] is selected from the DNS Server Auto Obtain and DNS Domain Name Auto Retrieval, the DNS Server Address and DNS Domain Name are automatically acquired.

3 Touch [OK].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

<From PageScope Web Connection>

✔ For the procedure to access the TCP/IP Setting screen on the display, see steps 1 through 3 of page 2-103.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start the PageScope Web Connection and call the TCP/IP Setting screen on the display.

2 Enter the address in the DNS Server box.

➔ If [Enable] is selected from the DNS Server Auto Obtain and DNS Domain Auto Obtain pull-down menus, the DNS Server Address and DNS Domain Name are automatically acquired.

3 Make the necessary settings.

4 Click [OK].

2.21 AppleTalk Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables making of the AppleTalk Settings.

Making the AppleTalk Setting

<From the Control Panel>

✔ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-93.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Network Settings screen on the display from the control panel.

2 Touch [AppleTalk Settings].

3 Make the necessary settings.

4 Touch [OK].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Network] tab.

3 Click [AppleTalk Setting] from the menu.

4 Make the necessary settings.

5 Click [OK].

2.22 E-Mail Setting Function

When access to the machine by the administrator of the machine through the Administrator Settings is authenticated, the machine enables setting of the SMTP Server (E-Mail Server).

Setting the SMTP Server (E-Mail Server)

<From the Control Panel>

✔ For the procedure to call the Network Settings screen on the display, see steps 1 and 2 of page 2-93.

✔ Do not leave the machine with the setting screen of Administrator Settings left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Administrator Settings.

1 Call the Network Settings screen on the display from the control panel.

2 Touch [E-Mail Settings].

3 Touch [E-Mail TX (SMTP)].

4 Make the necessary settings.

5 Touch [OK].

6 Touch [Close].

➔ If a message appears that prompts you to turn OFF and ON the main power switch, turn OFF and ON the main power switch. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

<From PageScope Web Connection>

✔ For the procedure to access the Admin Mode, see page 2-2.

✔ Do not leave the machine with the Admin Mode setting screen left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode.

1 Start PageScope Web Connection and access the Admin Mode.

2 Click the [Network] tab.

3 Click [E-mail Setting] ▸▸ [E-mail TX Setting (SMTP)] from the menu.

4 Make the necessary settings.

5 Click [OK].

3 User Operations

3 User Operations

3.1 User Authentication Function

When [ON (MFP)] or [External Server Authentication] (Active Directory) is set for Authentication Method of the Administrator Settings, the machine authenticates a user as an authorized user of this machine through the User Password that meets the Password Rules before he or she actually uses it. During the authentication procedure, the User Password entered for the authentication purpose appears as "*" or "●" on the display.

After authentication by a user is successful using the User Name and Password entered from the control panel with the ID & Print Setting function set in the machine, the user can automatically print his or her print data saved in the ID & Print User Box. Because printing occurs after user authentication is performed via the control panel of this machine, it is suitable for printing highly confidential documents.

When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

NOTICE

If [ON (MFP)] is set for the authentication method and [Pause] is set for a user or account by the administrator of the machine, that particular user or account cannot log onto the machine. For details, contact the administrator of the machine.

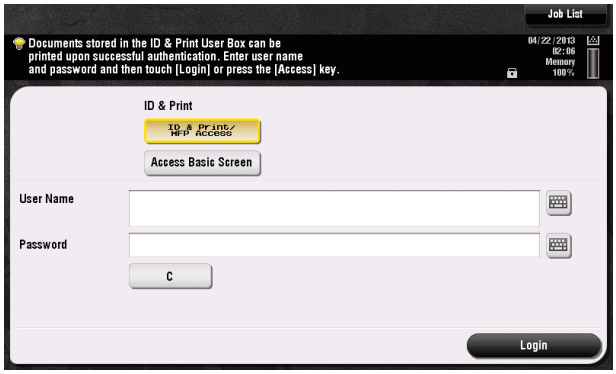
If a screen appears that warns that the job log has reached its upper limit, contact the administrator of the machine.

3.1.1 Performing user authentication

<From the Control Panel>

- ✔ Before operating the machine, the user him/herself should change the User Password from that registered by the administrator of the machine. For details of changing the User Password, see page 3-10. For details of User Name and User Password, ask the administrator of the machine.
- ✔ If the User Password is changed by the administrator of the machine during operation of this machine, the user him/herself should immediately change the User Password.
- ✔ Make absolutely sure that your User Password is not known by any other users.
- ✔ Do not leave the machine while you are in the user (account) operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user (account) operation mode.
- ✔ If any User Name not registered with this machine is authenticated through User Authentication when [External Server Authentication] (Active Directory) is set for Authentication Method, the User Name is automatically registered with this machine.

1 Touch the keyboard icon in the [User Name] field.



2 Enter the User Name and the Password from the keyboard.

➔ Touch [C] to clear the value entered.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

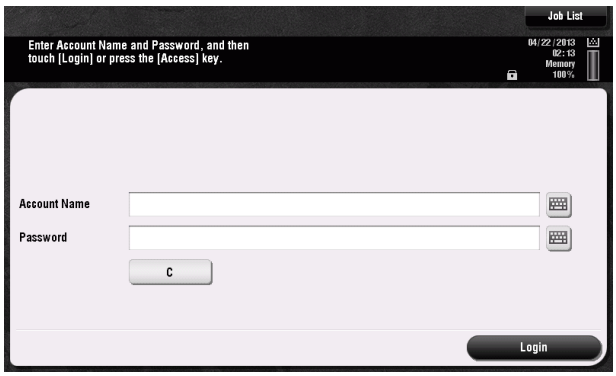
3 Touch [OK].

4 Touch [Access] or [Login]. If a document is stored in the ID & Print User Box, select the target logon method and then touch [Access] or [Login].

Login Method	Description
[ID & Print / MFP Access]	The user operation mode screen is called to the screen after the ID & Print document of the corresponding user is printed, but does not allow to login this machine.
[Access Basic Screen]	If [Access Basic Screen] is selected, only the ordinary login procedure is applicable and no ID & Print documents are printed.

➔ If a wrong User Name is entered, a message that tells that the authentication has failed appears. Enter the correct User Name.
➔ If a wrong User Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Password.
➔ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If a wrong User Password for the corresponding User Name entered is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.
➔ If there are two ore more ID & Print documents are involved, all of them will be printed. To select and print only a desired document, select [Access] or [Login] and select the desired document from those in the ID & Print User Box. For the detailed procedure to access the ID & Print document, see page 3-8.
➔ Go to step 9 if User Authentication only has been set, or "Synchronize" has been set for Synchronize User Authentication & Account Track. If the account to which the user belongs has not been registered by the administrator of the machine, however, Account Track becomes necessary even with [Synchronize] set for [Synchronize User Authentication & Account Track]. Account Track is, however, necessary only for the first time. Once any account is authenticated, that particular account is registered for Account Name. The machine can thereafter be used only through User Authentication. It should be noted that this function is valid only through operation from the control panel of the machine. In operation from PageScope Web Connection or application software, if Account Name is not registered, you cannot log onto the mode.

5 Touch the keyboard icon in the [Account Name] field.



6 Enter the Account Name and the Password from the keyboard.

➔ Touch [C] to clear the value entered.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

7 Touch [OK].

8 Touch [Access] or [Login].

➔ If a wrong Account Name is entered, a message that tells that the authentication has failed appears. Enter the correct Account Name.
➔ If a wrong Account Password is entered, a message that tells that the authentication has failed appears. Enter the correct Account Password.
➔ If the Enhanced Security Mode is set to [ON], the entry of a wrong Account Password is counted as unauthorized access. If a wrong Account Password for the corresponding Account Name entered is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

9 Touching [Access] will show the following screen.
To log off, select [Yes].

<From PageScope Web Connection>

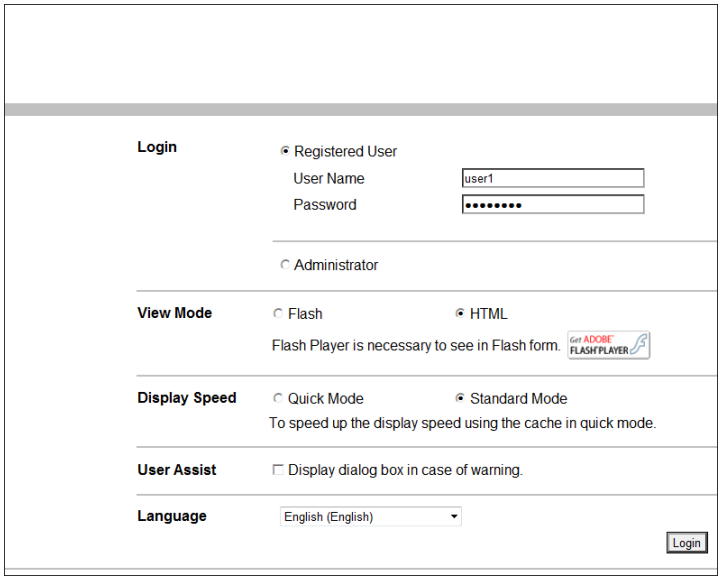
- ✔ Do not leave the machine while you are in the user (account) operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user (account) operation mode.
- ✔ If any User Name not registered with this machine is authenticated through User Authentication when [External Server Authentication] (Active Directory) is set for Authentication Method, the User Name is automatically registered with this machine.
- ✔ Different initial screens appear after you have logged on depending on the Customize setting made by the administrator or user. The descriptions herein given are concerned with the display screen set in [Device Information] of Information.

1 Start the Web browser.

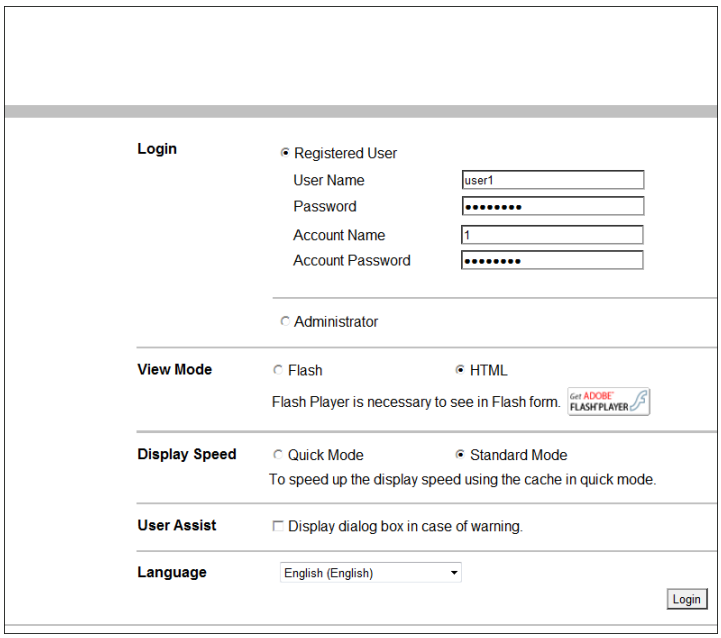
2 Enter the IP address of the machine in the address bar.

3 Press the [Enter] key to start PageScope Web Connection.

4 Click the Registered User radio button and enter the User Name and User Password.



➔ If Account Track has been set and [Do Not Synchronize] set for [Synchronize User Authentication & Account Track], also enter Account Name and Account Password.

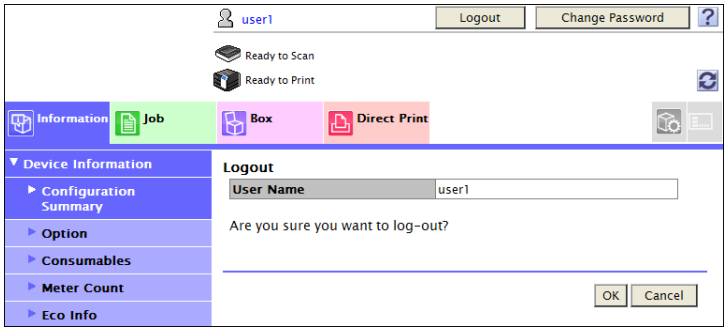


5 Click [Login].

➔ If a wrong User Password or Account Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Password or Account Password.

➔ If the Enhanced Security Mode is set to [ON], the entry of a wrong User/Account Password is counted as unauthorized access. If a wrong User/Account Password for the corresponding User/Account Name entered is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

6 Clicking [Logout] will show the following screen.
Click [OK] to log off from the user operation mode.



3.1.2 Accessing the ID & Print Document

If a user, whose document is stored in the ID & Print User Box, is authenticated by [Access] or [Login], he or she can gain access to the document in the ID & Print User Box.

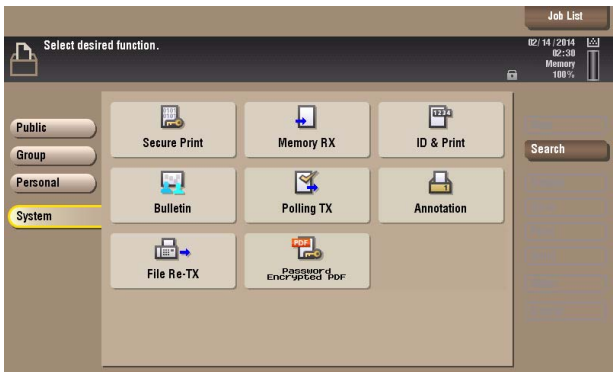
- ✔ For the logon procedure, see page 3-2.
- ✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
- ✔ Save the ID & Print document through the printer driver on the PC side. As in the ordinary user authentication procedure, enter the User Name and User Password in the printer driver on the PC side and then specify [ID & Print]. The password entered is displayed as "*." If the User Password does not correspond to the User Name entered, the ID & Print document is discarded without being saved. Entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the subsequent authentication operation is an access lock state and it is not possible to transmit the print job. As a result, the access lock state disables user authentication attempts from the control panel or PageScope Web Connection.
  To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.
- ✔ If an attempt is made to print or save a file by specifying a user name that contains ["] (a double quotation mark), a login error results and the machine cancels the print job.

1 Log on to the user operation mode through user authentication from the control panel.

2 Touch [Menu] ▸▸ [User Box].

3 Touch [System].

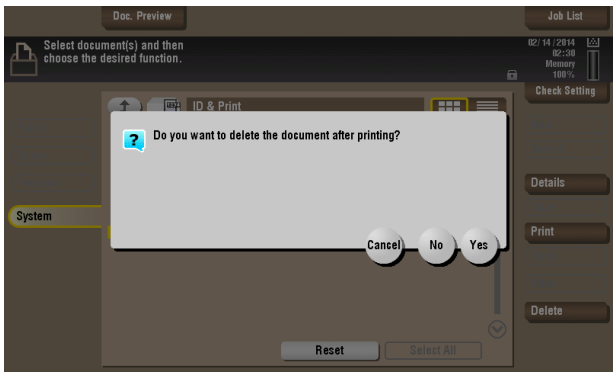
4 Touch [ID & Print].



5 Select the desired ID & Print document and touch [Print].

➔ To delete ID & Print document, select the specific document and touch [Delete].

6 To delete the document from the Box after the printing, select [Yes]. To leave the document as is, select [No].



3.2 Change Password Function

When [ON (MFP)] is set for Authentication Method of User Authentication, the machine permits each of all users who have been authenticated through User Authentication to change his or her User Password.

The User Password entered is displayed as "*" or "●."

Performing Change Password

<From the Control Panel>

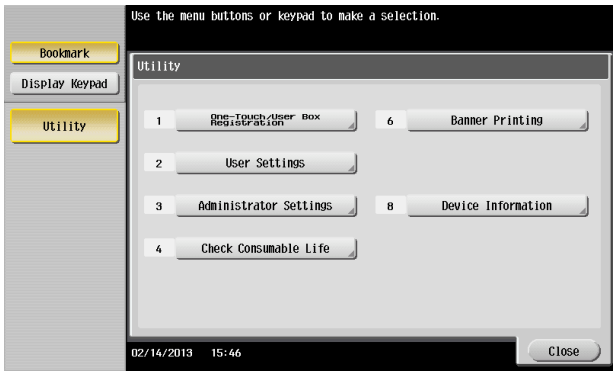
✔ For the logon procedure, see page 3-2.

✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

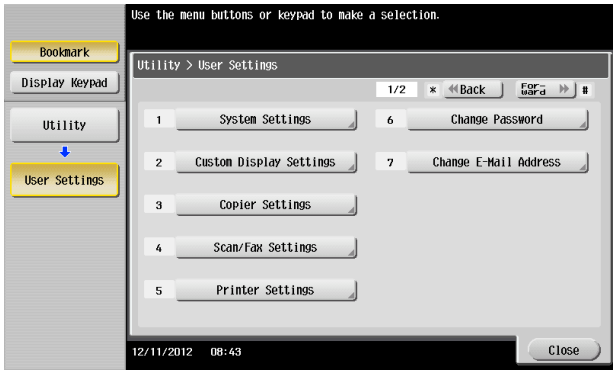
1 Log on to the user operation mode through User Authentication from the control panel.

2 Touch [Menu] ▸▸ [Utility].

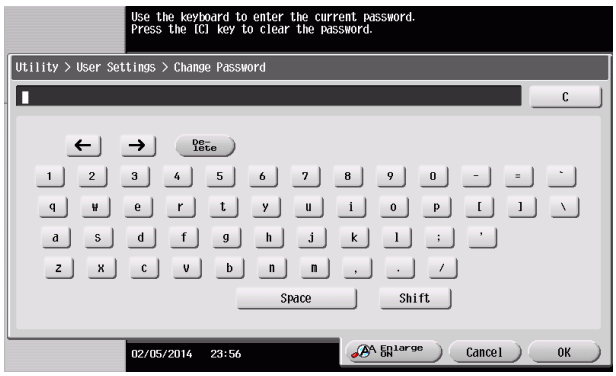
3 Touch [User Settings].



4 Touch [Change Password].



5 Enter the currently registered User Password from the keyboard.

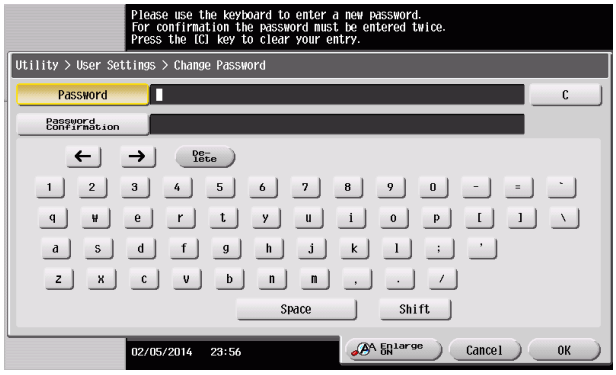


➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

6 Touch [OK].

➔ If a wrong User Password is entered, a message that tells that the User Password does not match appears. Enter the correct User Password.
➔ If the Enhanced Security Mode is set to [ON], the entry of a wrong User Password is counted as unauthorized access. If the current password is mistakenly entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the user authentication screen will reappear. A message then appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is now set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

7 From the keyboard, enter the new User Password.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the User Settings screen.

8 Touch [OK].

➔ If the entered User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-11.
➔ If the entered User Password does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.

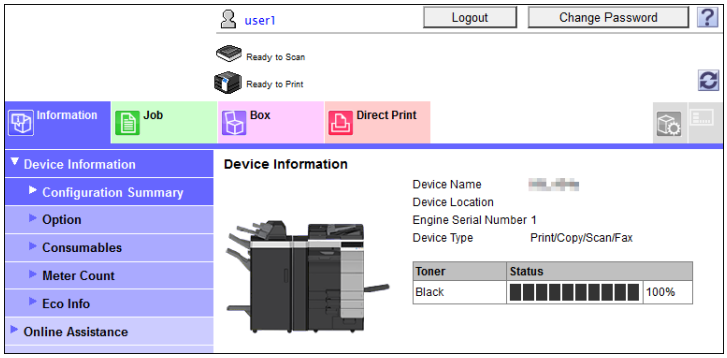
<From PageScope Web Connection>

✔ For the logon procedure, see page 3-2.

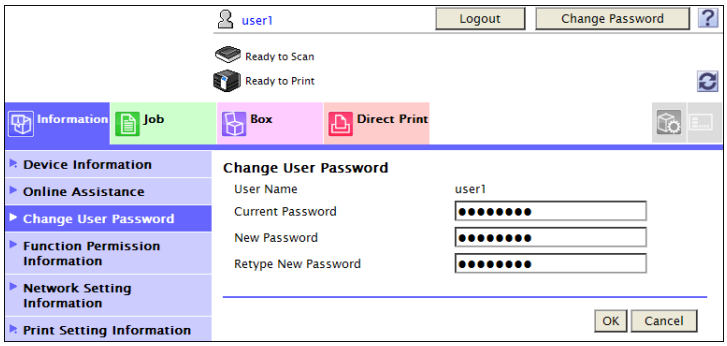
✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

1 Log on to the user operation mode through User Authentication from the PageScope Web Connection.

2 Click [Change Password].



3 Enter the currently registered User Password and a new User Password. Then, to make sure that you have entered the correct new password, enter the new User Password once again.



4 Click [OK].

➔ If a wrong User Password is entered in the "Current Password" box, a message that tells that the User Password does not match appears. Enter the correct User Password.

➔ If the entered User Password in the "New Password" box does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-11.

➔ If the entered User Password in the "New Password" box and "Retype New Password" box does not match, a message that tells that the User Password does not match appears. Enter the correct User Password.

5 Click [OK].

3.3 Secure Print Function

The Secure Print function allows a Secure Print document specified by a corresponding password from the PC to be used in the condition saved in the machine.

To access a Secure Print document, the machine authenticates a user as an authorized user of the Secure Print document file through the Secure Print Password that meets the Password Rules. The password entered is displayed as "*." When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

Accessing the Secure Print Document

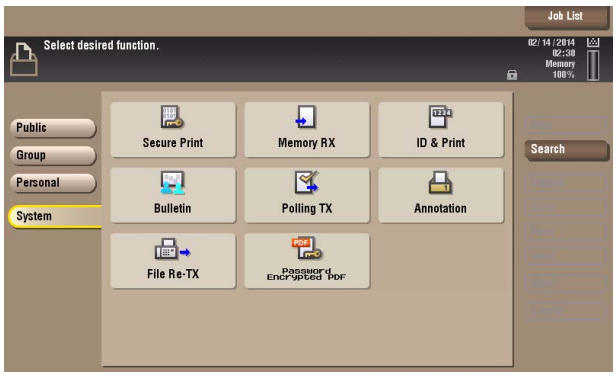
- ✔ For the logon procedure, see page 3-2.
- ✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.
- ✔ When the Enhanced Security Mode is set to [ON], go through User Authentication by entering the User Name and User Password registered in the machine through the printer driver of the PC. The password entered is displayed as "*." If the User Password does not correspond to the User Name entered, the Secure Print Job is discarded without being saved. Entry of a wrong User Password is counted as unauthorized access. If a wrong User Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the subsequent authentication operation is an access lock state and it is not possible to transmit the print job. As a result, the access lock state disables user authentication attempts from the control panel or PageScope Web Connection.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.
- ✔ Enter the Secure Print ID and password through the printer driver on the PC side. The password entered is displayed as "*."
- ✔ For the Secure Print Password, enter the password that meets the Password Rules. Any Secure Print document, the password for which does not meet the Password Rules, will not be saved in the machine. For details of the Password Rules, see page 1-11.
- ✔ If an attempt is made to print or save a file by specifying a user name that contains ["] (a double quotation mark), a login error results and the machine cancels the print job.

1 Log on to the user operation mode through User Authentication from the control panel.

2 Touch [Menu] ▸▸ [User Box].

3 Touch [System].

4 Touch [Secure Print].



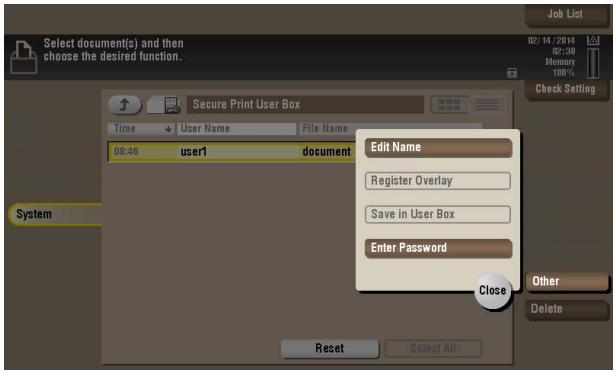
5 Enter the Secure Print ID from the keyboard.

➔ For the Secure Print ID, enter the one that has been set on the printer driver side.
➔ Touch [C] to clear the value entered last.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

6 Touch [OK].

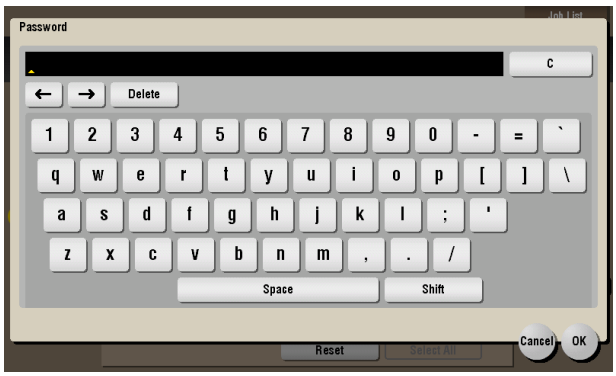
➔ If a wrong Secure Print ID is entered, the desired Secure Print document will not be displayed. Enter the correct Secure Print ID.

7 Select the desired Secure Print document and touch [Other] ▸▸ [Enter Password].



➔ Two or more Secure Print Documents can be selected at the same time.
➔ Touching [Select All] will select all Secure Print Documents having the same ID shown in the list.

8 Enter the Secure Print Password from the keyboard.



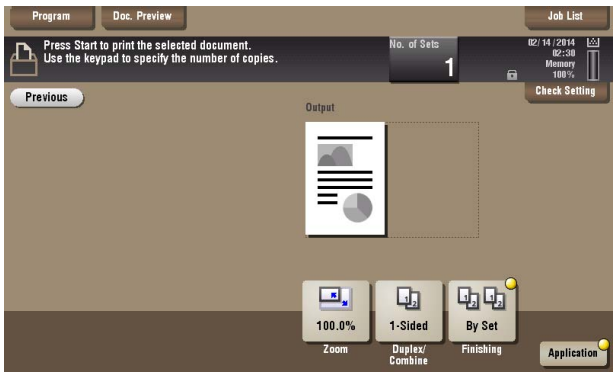
➔ Any Secure Print Password that does not meet the Password Rules is not accepted.
➔ For the Secure Print Password, enter the one that has been set on the printer driver side.
➔ Touch [C] to clear the value entered last.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

9 Touch [OK].

➔ If a wrong Secure Print Password is entered, a message that tells that the authentication has failed appears. Enter the correct Secure Print Password.
➔ If two or more Secure Print documents have been selected in step 7, the machine counts as unauthorized access any Secure Print document, the Secure Print Password of which is a mismatch.
➔ If the Enhanced Security Mode is set to [ON], entry of a wrong Secure Print Password is counted as unauthorized access. If a wrong Secure Print Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, disabling access to the Secure Print document. To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

10 Touch [Print].

11 Check the details of the document and press the [Start] key.



➔ If two or more Secure Print documents, each having an identical Secure Print ID and Secure Print Password, have been saved, multiple Secure Print documents can be printed at once.

➔ Touch [Previous] to go back to the previous screen.

3.4 User Box Function

For all users who have been authenticated through User/Account Authentication, the machine enables the operation of registering and changing the User Box. It also enables the operation of acquiring or printing image files saved in the User Box and sending of S/MIME encrypted image files.

User Box creates a User Box in the HDD as a space for storing an image file. User Box is available in three different types: Personal User Box which only the user who has logged on through User Authentication can use; Public User Box that is shared among two or more users who have previously registered; and Group User Box that can be used by the user who has logged on through Account Authentication. Up to 1,000 User Boxes can be registered.

When a user accesses a Public User Box, he or she is authenticated by a box password that meets the Password Rules. The password entered for the authentication purpose appears as "*" or "●" on the display.

When the Enhanced Security Mode is set to [ON], the number of times in which authentication fails is counted.

Reference

- If a document is saved in the Copy mode, Fax/Scan mode, or User Box mode selected from the control panel, or from an external memory, by specifying a User Box number that has not been registered, a Personal User Box owned by the user who logged on through User Authentication or a Group User Box owned by the account to which the user who logged on through User Authentication belongs is automatically created. No Public User Boxes are automatically created.
- When a document is saved in a box with a box number yet to be registered specified from the PC, the Personal User Box owned by the user who logged on through User Authentication is automatically registered.
- To use the external memory function, settings must be made by the administrator of the machine. For details, contact the administrator of the machine.
- If Account Track has not been enabled, Group User Box cannot be created.

3.4.1 Setting the User Box

<From the Control Panel>

✔ For the logon procedure, see page 3-2.

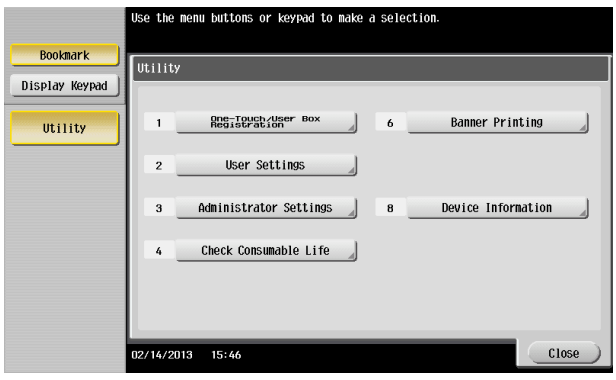
✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

✔ For the procedure to change the User Box setting, see page 3-23.

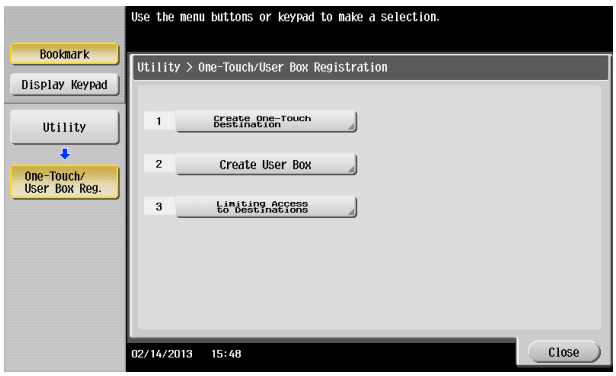
1 Log on to the user operation mode through User Authentication from the control panel.

2 Touch [Menu] ►► [Utility].

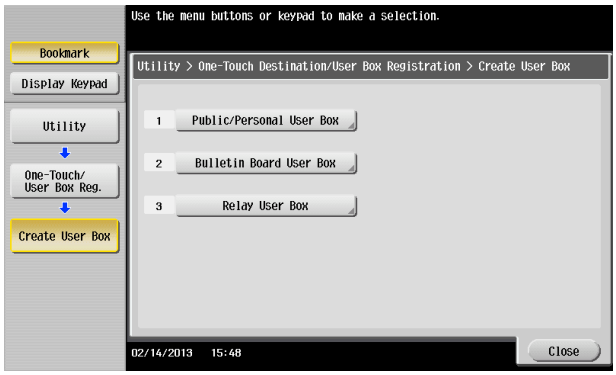
3 Touch [One-Touch/User Box Registration].



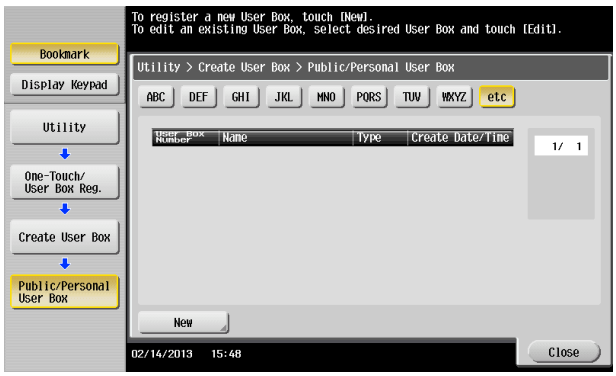
4 Touch [Create User Box].



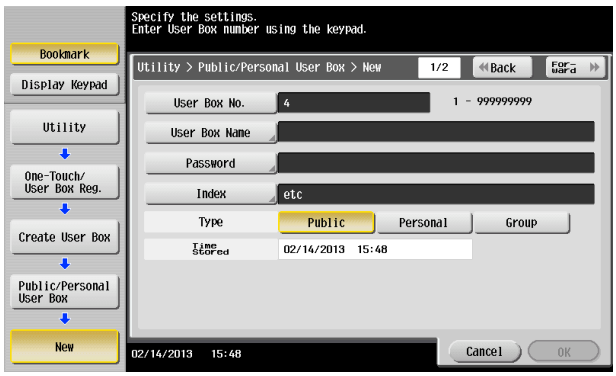
5 Touch [Public/Personal User Box].



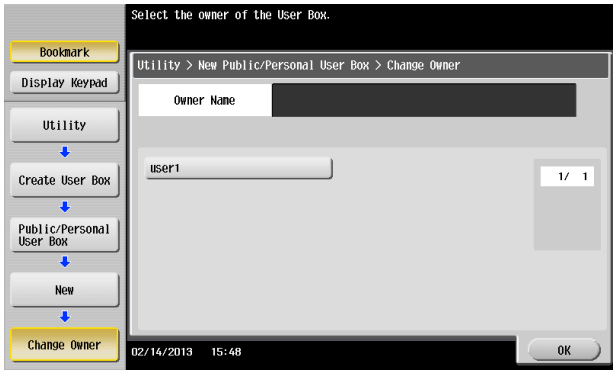
6 Touch [New].



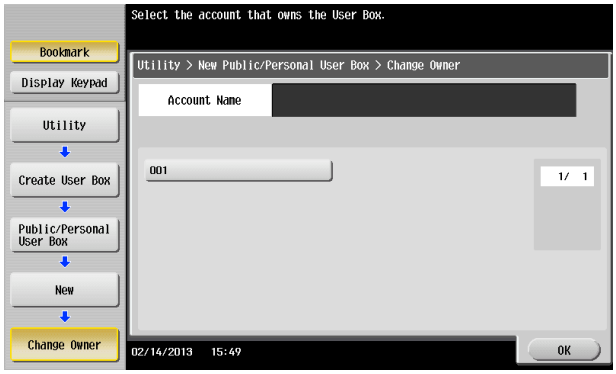
7 Select the User Box type.



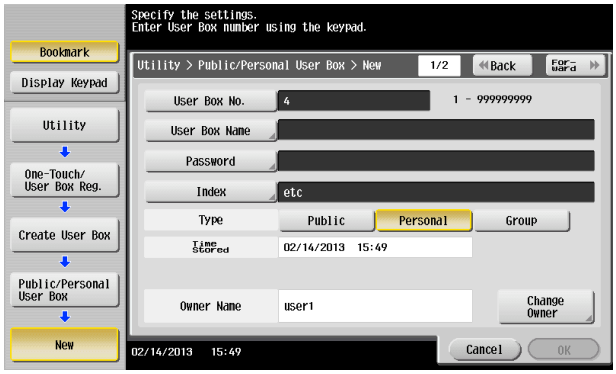
➔ When [Personal] is selected, [Change Owner] is displayed. Then, select the desired owner name. The default value of [Owner Name] is the user who has currently logged on to the function.



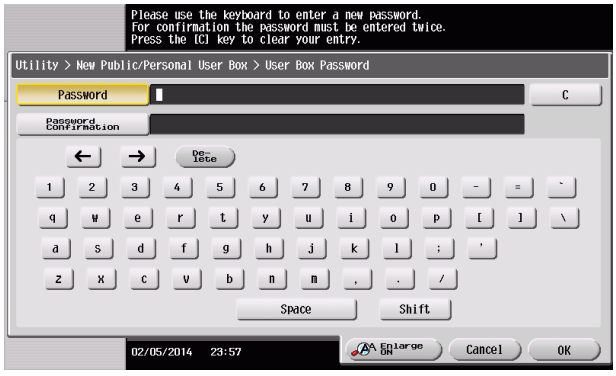
➔ When [Group] is selected, [Change Account Name] is displayed. Then, select the desired account name. The default value of [Account Name] is the account to which the user who has currently logged on to the function belongs.



8 Touch [Password].



9 Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].

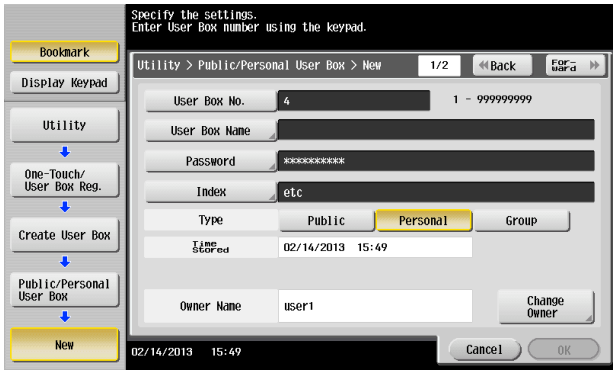


➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

10 Touch [OK].

➔ If the User Box Type is set to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.
➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Passwords.

11 Make the necessary settings.



➔ A User Box No. that already exists cannot be redundantly registered.
➔ If no Name has been registered, [OK] cannot be touched. Be sure to register the Name.

12 Touch [OK].

<From PageScope Web Connection>

✔ For the logon procedure, see page 3-2.

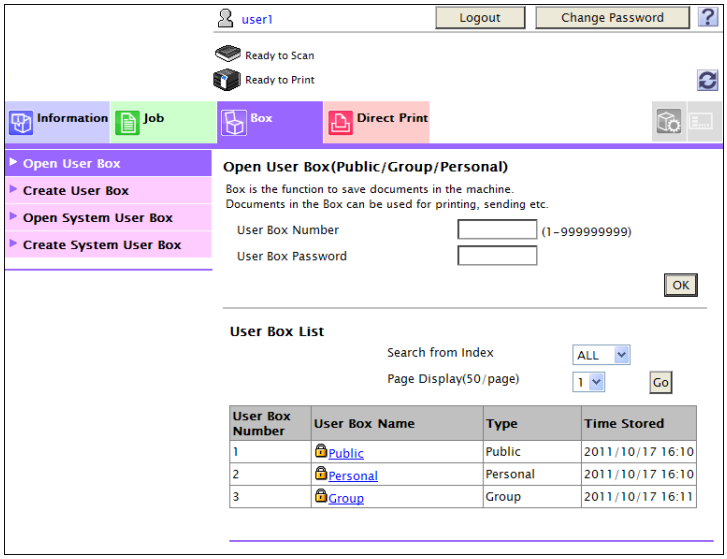
✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

✔ For the procedure to change the User Box setting, see page 3-23.

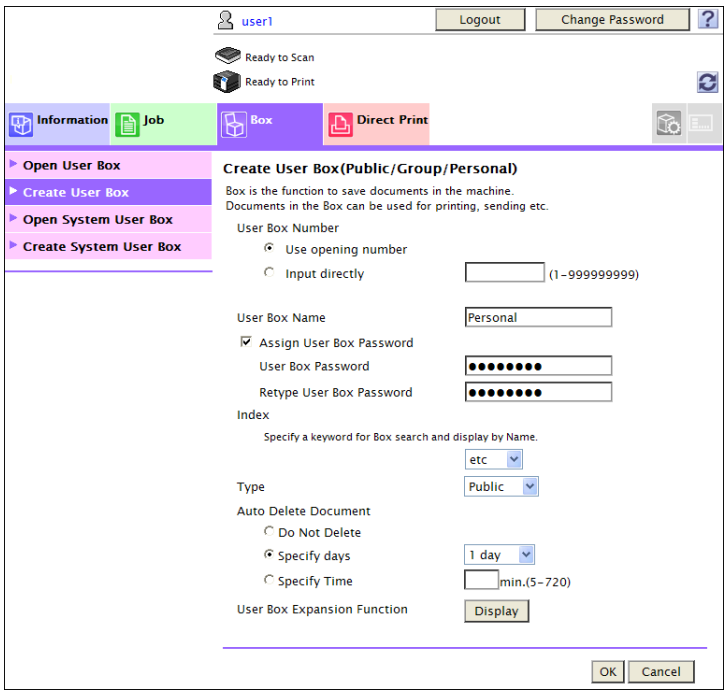
1 Log on to the user operation mode through User Authentication from the PageScope Web Connection.

2 Click the [Box] tab

3 Click [Create User Box] from the menu.



4 Make the necessary settings.



➔ Be sure to enter the User Box Number, User Box Name, User Box Password, and Retype User Box Password.

➔ A User Box Number that already exists cannot be redundantly registered.

➔ If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.

➔ If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.

5 Click [OK].

➔ If the User Box Type is set to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.

➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

➔ If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.

➔ If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.

➔ If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.

➔ If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.

6 Check the message that tells that the setting has been completed. Then, click [OK].

3.4.2 Changing the user/account attributes and box password

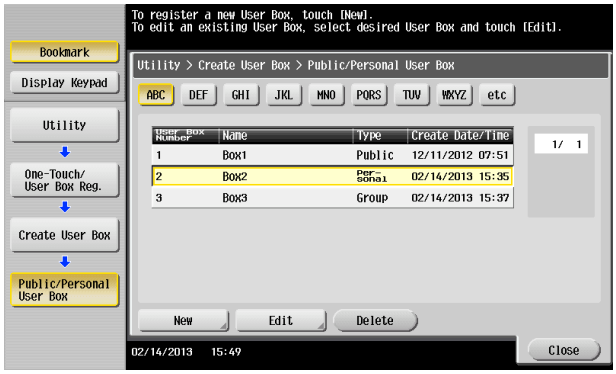
<From the Control Panel>

✔ For the procedure to call the User Box screen to the display, see steps 1 through 5 of page 3-17.

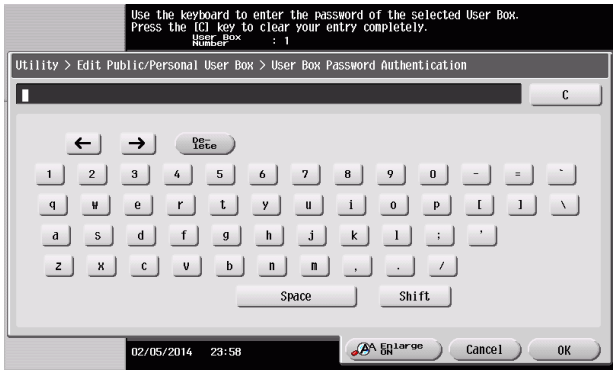
✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

1 Call the User Box screen to the display from the control panel.

2 Select the desired User Box and touch [Edit].



3 Enter the currently set User Box Password from the keyboard.



➔ Touch [C] to clear all characters.

➔ Touch [Delete] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the previous screen.

4 Touch [OK].

➔ If a wrong User Box Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Box Password.

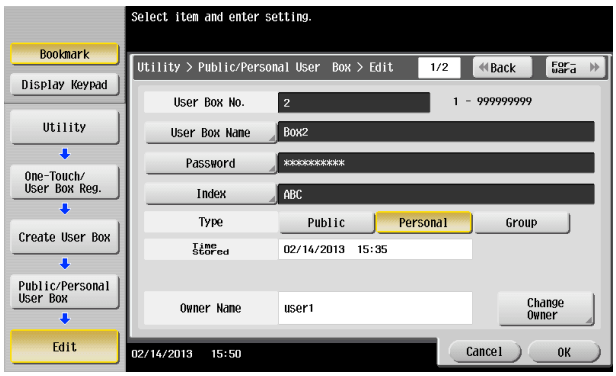
➔ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the screen of step 2 reappears and the machine is set into an access lock state.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

➔ To change the User Box Type, perform steps 5 through 8.

➔ To change the owner user or owner account, perform steps 6 through 8.

➔ To change the User Box Password, go to step 9.

5 Select the User Box Type.

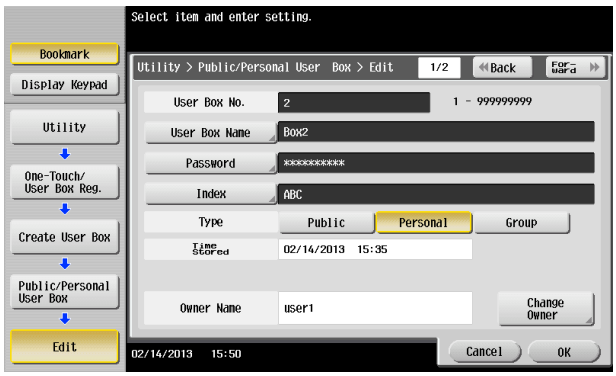


➔ [Change Owner] appears if the Box Type is changed to [Personal]. Select the desired owner name.

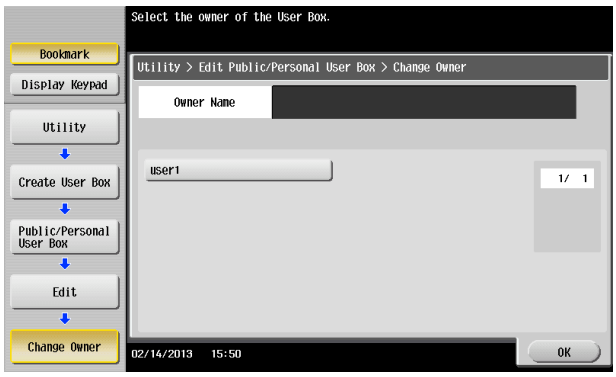
➔ [Change Account Name] appears if the Box Type is changed to [Group]. Select the desired account name.

➔ If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.

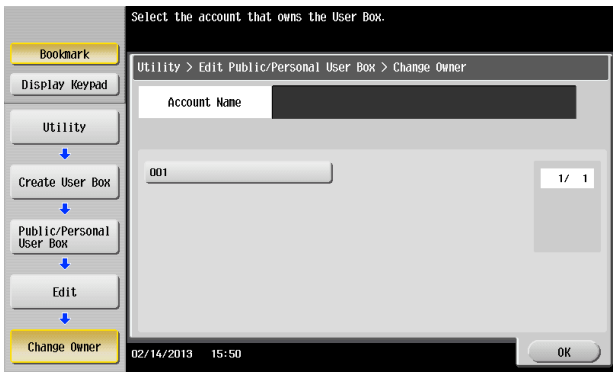
6 Touch [Change Owner] if the box type is [Personal] and touch [Change Account Name] if the box type is [Group].



7 For [Change Owner], select the desired owner name.

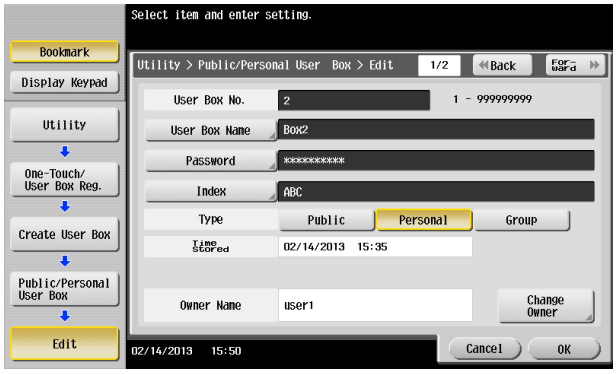


➔ For [Change Account Name], select the desired account name.



8 Touch [OK].

9 Touch [Password].



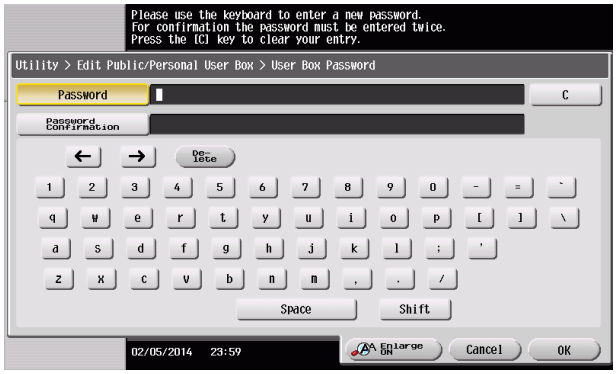
10 Enter the currently set User Box Password from the keyboard.

➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the previous screen.

11 Touch [OK].

➔ If a wrong User Box Password is entered, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.
➔ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, the screen of step 2 reappears and the machine is set into an access lock state.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

12 Enter the new User Box Password from the keyboard.
To prevent entry of a wrong password, enter the password again in [Password Confirmation].



➔ Touch [C] to clear all characters.
➔ Touch [Delete] to delete the last character entered.
➔ Touch [Shift] to show the upper case/symbol screen.
➔ Touch [Cancel] to go back to the screen shown in step 9.

13 Touch [OK].

➔ If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.
➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

14 Touch [OK].

<From PageScope Web Connection>

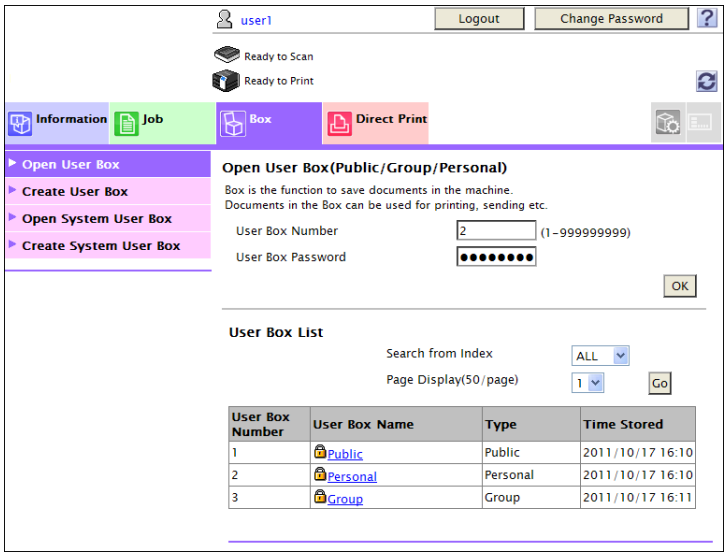
✔ For the logon procedure, see page 3-2.

✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

1 Log on to the user operation mode through User Authentication from the PageScope Web Connection.

2 Click the [Box] tab.

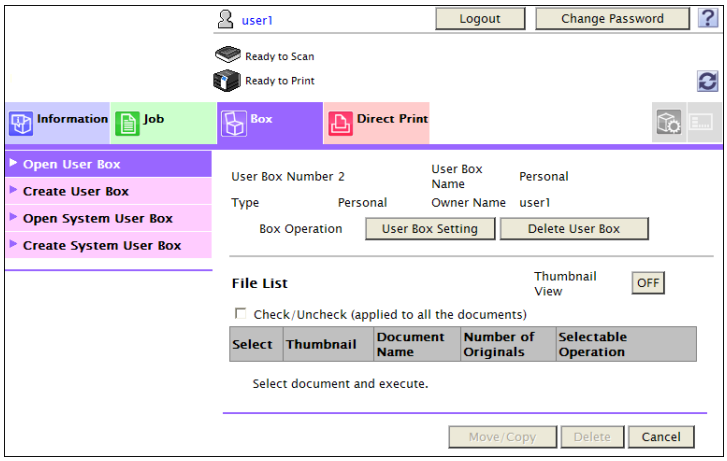
3 Enter the User Box Number and User Box Password of the desired User Box or click the desired User Box on the box list and enter the User Box Password.



➔ If a wrong User Box Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Box Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

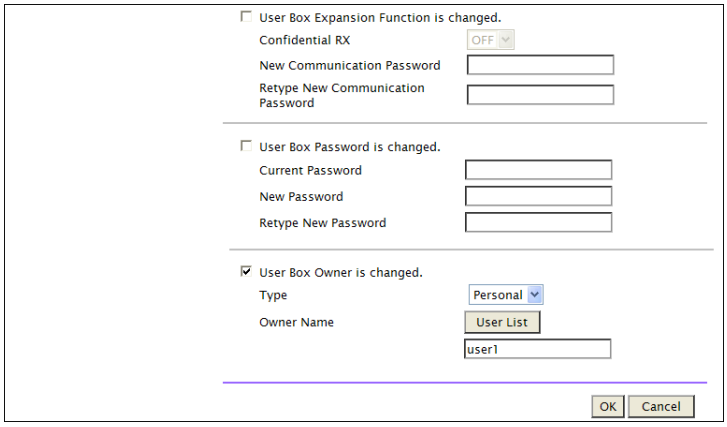
4 Click [User Box Setting].



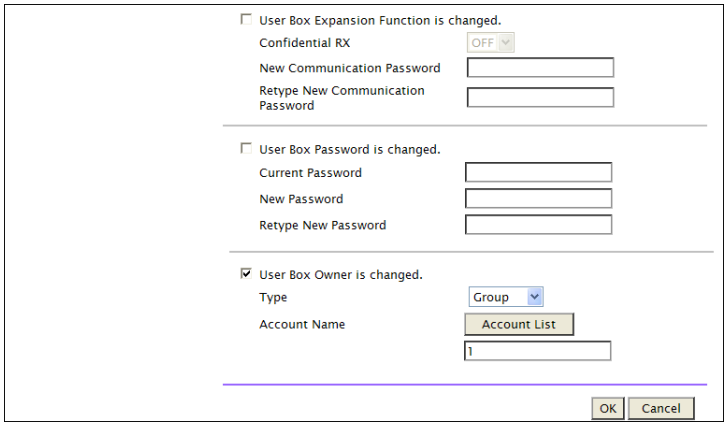
➔ Go to step 6 to change the User Box Password.

➔ To delete a User Box, click [Delete User Box]. A confirmation message appears. Click [OK] to delete the specified User Box.

5 Click the "User Box Owner is changed." check box and change the user attributes of the box.



➔ The following screen appears if the account attributes are to be changed.



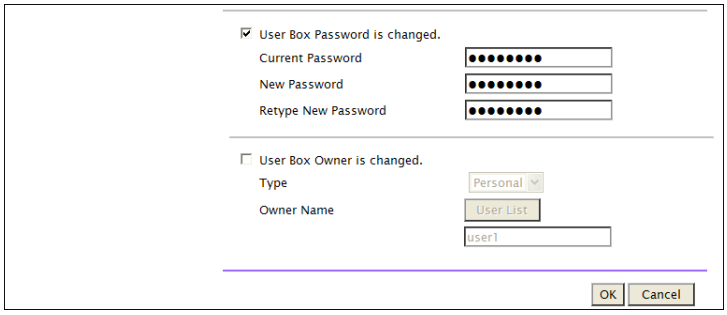
➔ If [Personal] is selected from the User Box Type pull-down menu, click [User List] and select the user from the registered user list. Or, directly enter in the "Owner Name" box the previously registered User Name.

➔ If [Group] is selected from the User Box Type pull-down menu, click [Account List] and select the account from the registered account list. Or, directly enter in the "Account Name" box the previously registered Account Name.

➔ If the "User Box Owner is changed." check box is not clicked, the changes made will not be validated. If the changes need to be made, make sure that the "User Box Owner is changed." check box has been clicked.

➔ To change the User Box Type, click the User Box Type pull-down menu and select the desired User Box Type.

6 Click the "User Box Password is changed." check box and enter the User Box Password.



➔ In the "Current Password" box, enter the currently set User Box Password.

7 Click [OK].

➔ If a wrong current User Box Password is entered, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

➔ If the User Box Type is changed to [Public], set a User Box Password that meets the Password Rules. For details of the Password Rules, see page 1-11.

➔ If the entered User Box Password does not match, a message that tells that the User Box Password does not match appears. Enter the correct User Box Password.

➔ If no Owner Name is entered, a message appears that tells that no Owner Names have been entered. Enter the correct Owner Name.

➔ If a user name not registered with the machine is entered in the "Owner Name" box, a message appears that tells that the Owner Name entered in the box is illegal. Enter the correct Owner Name.

➔ If no Account Name is entered, a message appears that tells that no Account Names have been entered. Enter the correct Account Name.

➔ If an account name not registered with the machine is entered in the "Account Name" box, a message appears that tells that the Account Name entered in the box is illegal. Enter the correct Account Name.

8 Click [OK].

3.4.3 Accessing the User Box and User Box file

<From the Control Panel>

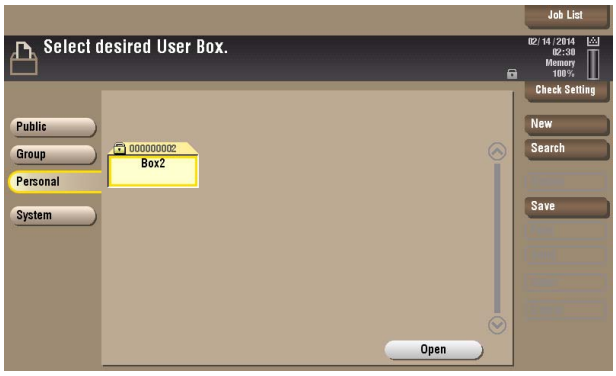
✔ For the logon procedure, see page 3-2.

✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

1 Log on to the user operation mode through User Authentication from the control panel.

2 Touch [Menu] ▸▸ [User Box].

3 Select the desired User Box and touch [Open].



➔ To save a new document, select [Save].

4 Enter the User Box Password from the keyboard.

➔ Touch [C] to clear the value entered last.

➔ Touch [Delete] to delete the last character entered.

➔ Touch [Shift] to show the upper case/symbol screen.

➔ Touch [Cancel] to go back to the previous screen.

5 Touch [OK].

➔ If a wrong User Box Password is entered, a message that tells that the authentication has failed appears. Enter the correct User Box Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

6 Select the desired file from each tab.

7 Select the desired function.

Different functions can be performed on different types of files stored in the User Boxes.
See the table given below for the relation between the file type and functions that can be performed.

File Type	Functions that can be Performed
Copy job files	Print, Send, Combine, Combine TX, Edit Name, Re-order, Copy, Edit Document, Save to External Memory, Delete
Print job files	Print, Send, Combine, Combine TX, Edit Name, Re-order, Copy, Edit Document, Save to External Memory, Delete
Scan job files	Print, Send, Combine, Combine TX, Edit Name, Re-order, Copy, Edit Document, Save to External Memory, Delete
Fax job files	Print, Send, Combine, Combine TX, Edit Name, Re-order, Copy, Edit Document, Save to External Memory, Delete

➔ If the destination is to be specified using the corresponding one-touch key for executing [Fax] or [Fax TX] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.

➔ If the destination is to be specified through direct input for executing [Fax] or [Fax TX] from the control panel, always check that the destination is correct to make sure that the data is sent to the correct destination.

➔ To delete the file, select the specific document and touch [Delete].

➔ To save a file in External Memory, select the specific document and touch [Other] ▸▸ [Save to External Memory].

8 Press the [Start] key.

<From PageScope Web Connection>

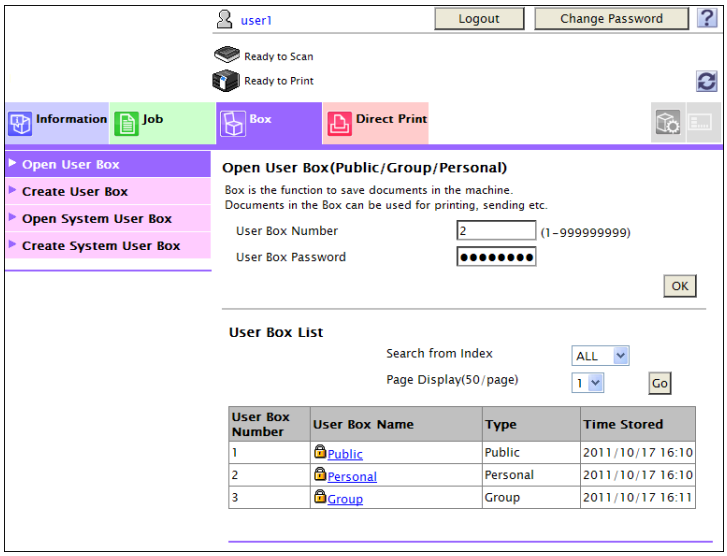
✔ For the logon procedure, see page 3-2.

✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

1 Log on to the user operation mode through User Authentication from the PageScope Web Connection.

2 Click the [Box] tab.

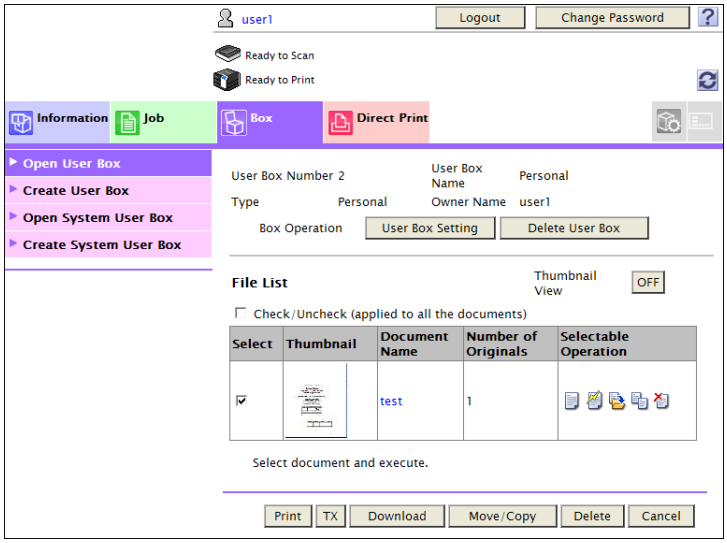
3 Enter the User Box Number and User Box Password of the desired User Box or click the desired User Box on the box list and enter the User Box Password.



➔ If a wrong User Box Password is entered, a message that tells that the authentication has failed appears. Enter the User Box Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong User Box Password is counted as unauthorized access. If a wrong User Box Password is entered a predetermined number of times (once to three times) or more set by the administrator of the machine, a message appears that tells that authentication has not been successful for any subsequent operation for authentication. The machine is then set into an access lock state, rejecting any more logon attempts.
To cancel the access lock state, the administrator of the machine must perform the Release Setting. Contact the administrator of the machine.

4 Select the document and perform the desired function.



➔ Different functions can be performed on different types of operation menu.
See the table given below for the relation between the menu type and functions that can be performed.

File Type	Functions that can be Performed
Copy job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete
Print job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete
Scan job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete
Fax job files	Print, TX, Combine, Combine, Download, Move, Copy, Delete

➔ If [Delete] is selected in step 4, a confirmation message appears. Click [OK] to delete the specified file.

3.4.4 Sending S/MIME box files

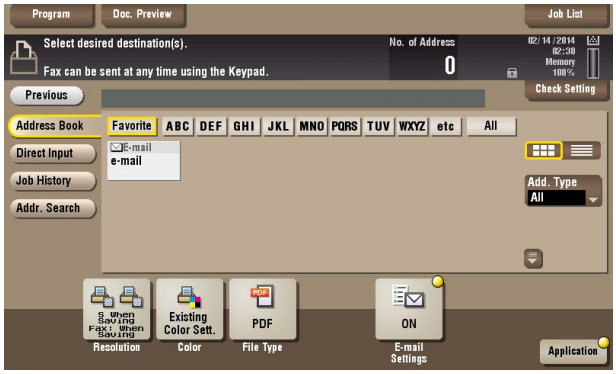
✔ For the procedure to call the Use Document screen to the display, see steps 1 through 5 of page 3-30.

✔ Do not leave the machine while you are in the user operation mode. If it is absolutely necessary to leave the machine, be sure first to log off from the user operation mode.

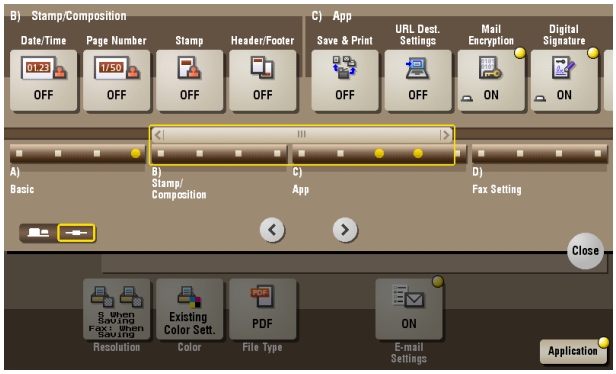
1 Call the Use Document screen to the display from the control panel.

2 Select the file to be sent and click [Send].

3 Touch [Application].



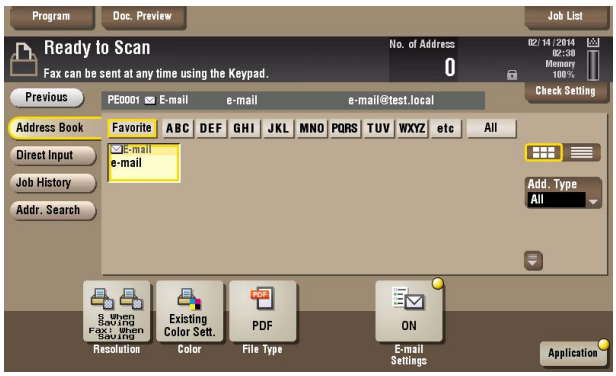
4 Select [Mail Encryption] and touch [Close].



➔ To select [Mail Encryption], the administrator of the machine must make the S/MIME settings in advance.

➔ If [Mail Encryption] is selected after the destination has been set, the set destination is canceled, making it necessary to set the destination once again.

5 Select the destination and press the [Start] key.



➔ To select the destination, the administrator of the machine must register the certificate with the destination in advance.

➔ An error message appears if the registered certificate is invalid, e.g., its validity is expired. Do not send the file in this case. The administrator of the machine is now required to register a valid certificate. Contact the administrator of the machine.

4 Application Software

4 Application Software

4.1 PageScope Data Administrator

PageScope Data Administrator is an application for management purpose that allows the authentication, destination and network functions of the machine to be edited or registered from a PC connected over the network.

It allows the authentication, destination and network setting list to be downloaded in your PC, the data in the list to be edited on the PC, and then the data to be written in the machine.

A destination list of file formats including XML, CSV, TAB, LDIF, and Lotus Notes Structured Text can be downloaded. A destination list can also be downloaded by searching through or browsing destinations using the LDAP protocol for a directory server such as Active Directory.

NOTICE

Make sure that none of the general users of the machine will know the Administrator Password.

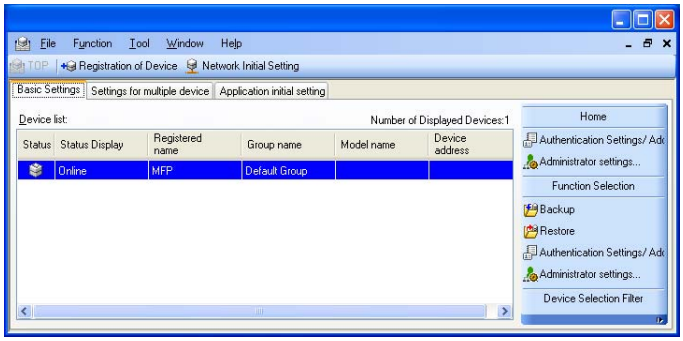
If the Administrator Password is forgotten, it must be set again by the Service Engineer. Contact your Service Representative.

4.1.1 Accessing from PageScope Data Administrator

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

1 Start the PageScope Data Administrator.

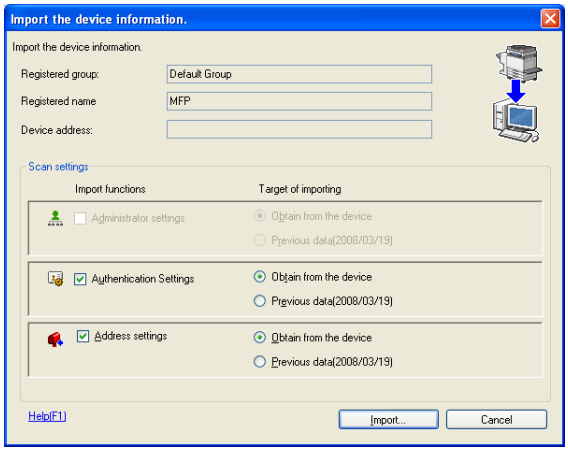
2 Select this machine from Device List and click [Authentication Settings/Address Settings] or [Administrator settings].



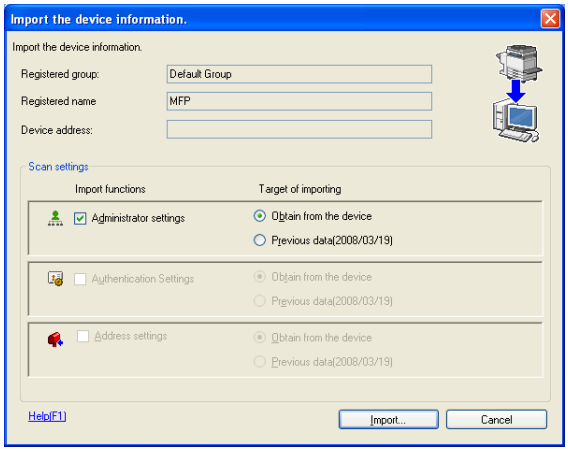
➔ Select [Authentication Settings/Address Settings] to edit or register the authentication or destination function of the machine, and select [Administrator settings] to edit or register the network function of the machine.

3 Check the settings on the "Import device information" screen and click [Import].

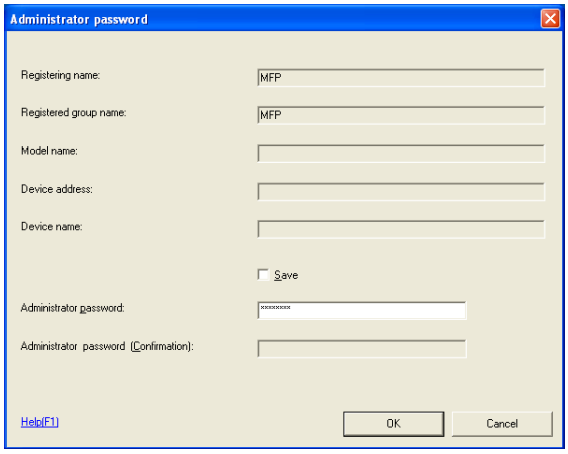
➔ The following screen appears if [Authentication Settings/Address Settings] is selected in step 2.



➔ The following screen appears if [Administrator settings] is selected in step 2.



4 Type the Administrator Password registered in the machine and click [OK].



➔ If the "Save" check box has been selected, the Administrator Password entered is stored in the PC being used. If you do not want the Administrator Password stored, clear the "Save" check box.

➔ If a wrong Administrator Password is entered, a message appears that tells that there is a mismatch in the passwords. Enter the correct Administrator Password.

➔ If the "Save" check box is selected, enter the 8-digit Administrator Password once again to make sure that the Administrator Password has been entered correctly.

➔ If a wrong Administrator Password is entered for confirmation, a message appears that tells that there is a mismatch in the Administrator Password. Enter the correct Administrator Password.

➔ If the Enhanced Security Mode is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) or more set by the Administrator of the machine, a message appears that tells that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.

5 Check the data displayed on the SSL certificate check screen and click [Yes].

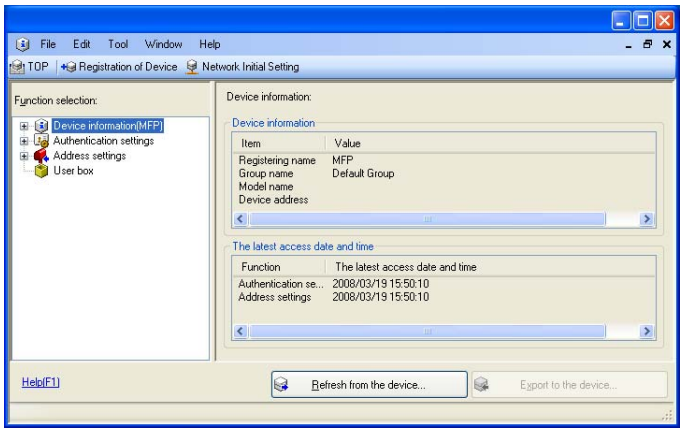
4.1.2 Setting the user authentication method

✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

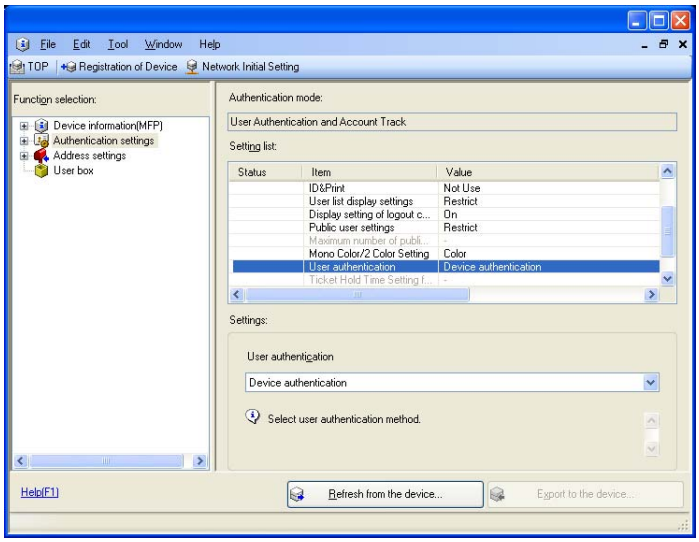
✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.

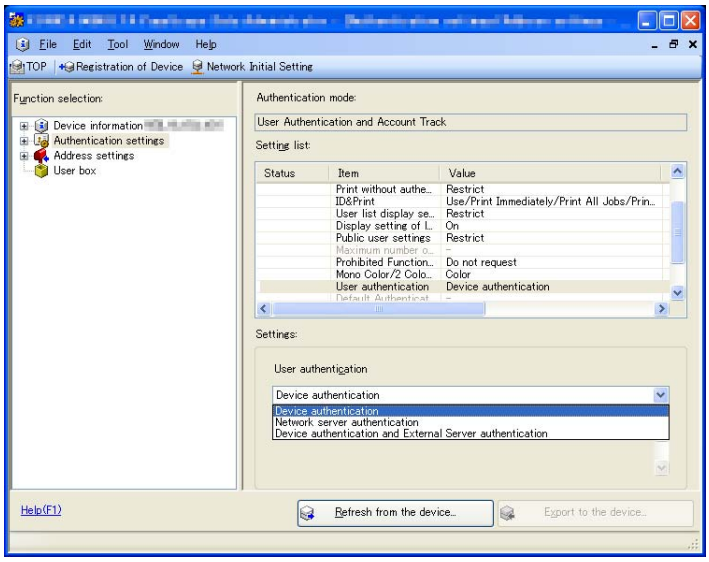
2 Click [Authentication settings].



3 Click [User authentication].



4 From the pull-down menu of User authentication, select the user authentication method.



➔ To change the user authentication method from "Device authentication" to "Network server authentication," it is necessary first to register the domain name of Active Directory on the machine side.

➔ If "Network server authentication" is selected, "Active Directory" must invariably be selected.

5 Click [Export to the device].

➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

➔ If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

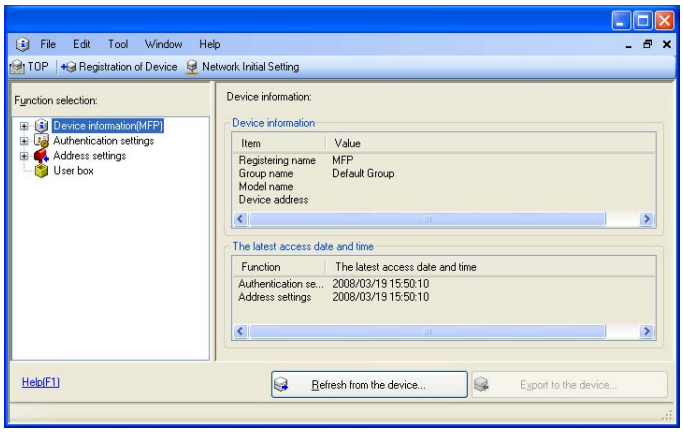
4.1.3 Changing the authentication mode

✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

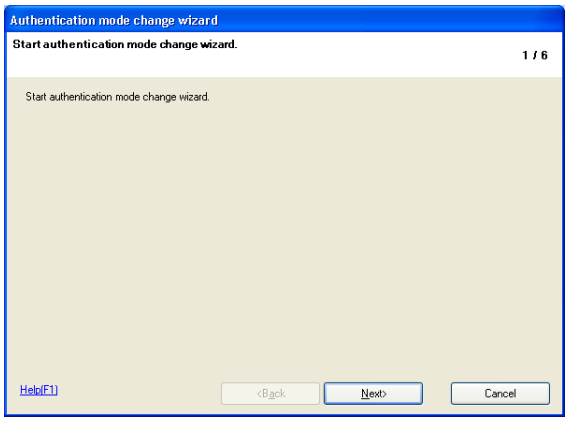
1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.

2 Click [Authentication settings].

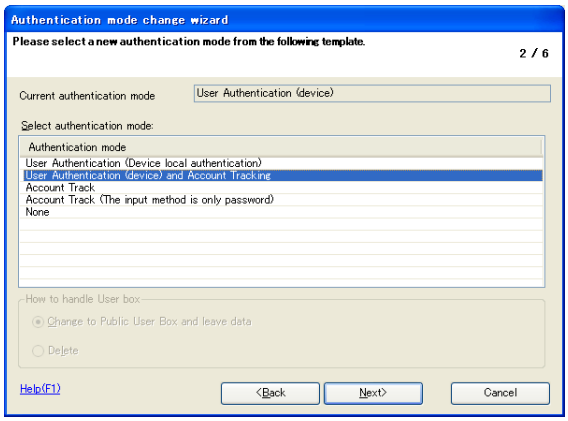


3 From [Edit] on the tool bar, select [Authentication] and click [Change authentication mode].

4 Click [Next].

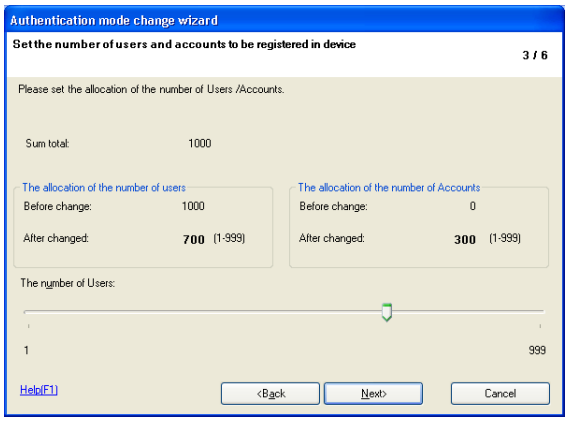


5 Select the specific [Authentication mode] to be changed and click [Next].

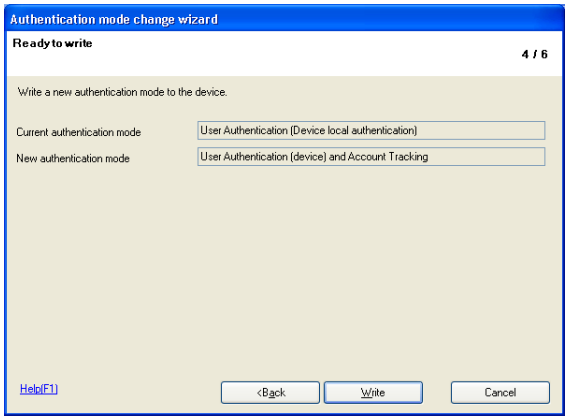


➔ Changing the Account Track setting erases all user and account information data that has previously been registered. At this time, Personal User Boxes owned by the users who are deleted and Group User Boxes owned by the accounts that are deleted may be deleted or changed to Public User Boxes.
If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

➔ If [User Authentication (device) and Account Tracking] is selected, set [The ratio of the number of Users] and [The ratio of the number of Accounts].



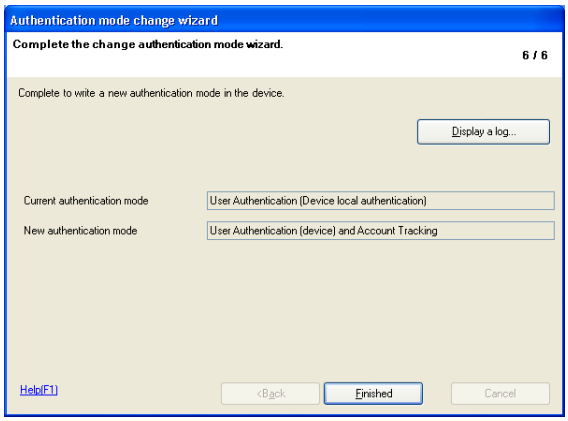
6 Verify the new authentication mode and click [Write].



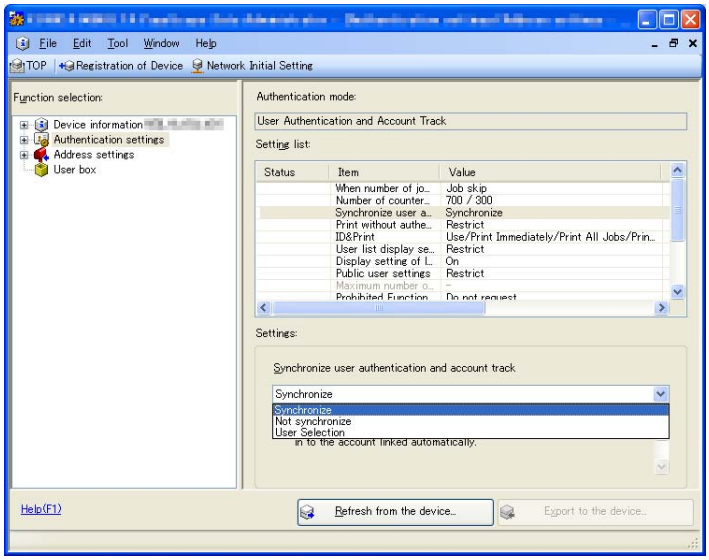
➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

➔ If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

7 Click [Finished].



➔ If [User Authentication (device) and Account Tracking] is selected in step 5, [Synchronize] is set for "Synchronize user authentication and account track." If [Synchronize] is not desired, select the desired method and execute [Export to the device] once again.



4.1.4 Making the user settings

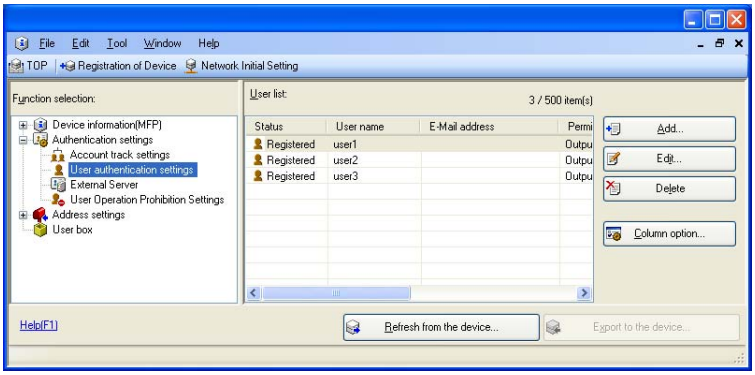
✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.

2 Click the Authentication settings expand button.

3 Click [User authentication settings].

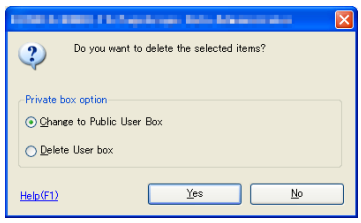


4 Select the desired function.

➔ To register the user, click [Add].

➔ To change data registered for the user, click [Edit].

➔ To delete the user, click [Delete]. The following screen appears if the user to be deleted owns a Personal User Box. Select whether to delete the Personal User Box or change it to the Public User Box.



➔ If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

➔ If the User Password does not meet the Password Rules, a message that tells that the entered User Password cannot be used appears. Enter the correct User Password. For details of the Password Rules, see page 1-11.

➔ If the User Name has not been entered, a message appears that tells that the User Name is yet to be entered. Click [OK] and enter the User Name.

➔ A User Name that already exists cannot be redundantly registered.

5 Click [OK].

6 Click [Export to the device].

➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

➔ If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.5 Making the account settings

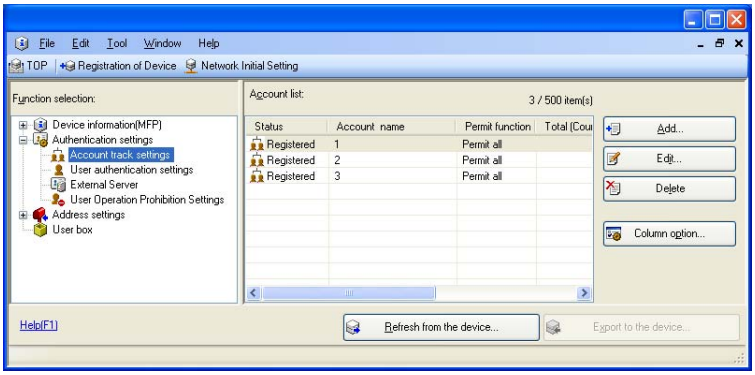
✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.

2 Click the Authentication settings expand button.

3 Click [Account track settings].

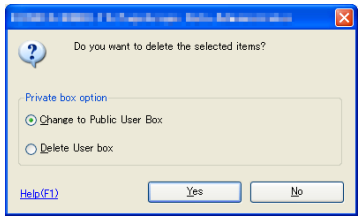


4 Select the desired function.

➔ To register the account, click [Add].

➔ To change data registered for the account, click [Edit].

➔ To delete the account, click [Delete]. The following screen appears if the account to be deleted owns a Group User Box. Select whether to delete the Group User Box or change it to the Public User Box.



➔ If the boxes are changed to Public User Boxes and if the password set for a particular box before this change does not meet the Password Rules, no access can be made to the Public User Box, to which that specific box was changed. In this case, the administrator must first newly set a password that meets the Password Rules. For details of the Password Rules, see page 1-11.

➔ If the Account Password does not meet the Password Rules, a message that tells that the entered Account Password cannot be used appears. Enter the correct Account Password. For details of the Password Rules, see page 1-11.

➔ If the Account Name has not been entered, a message appears that tells that the Account Name is yet to be entered. Click [OK] and enter the Account Name.

➔ An Account Name that already exists cannot be redundantly registered.

5 Click [OK].

6 Click [Export to the device].

➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

➔ If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.6 Registering the certificate

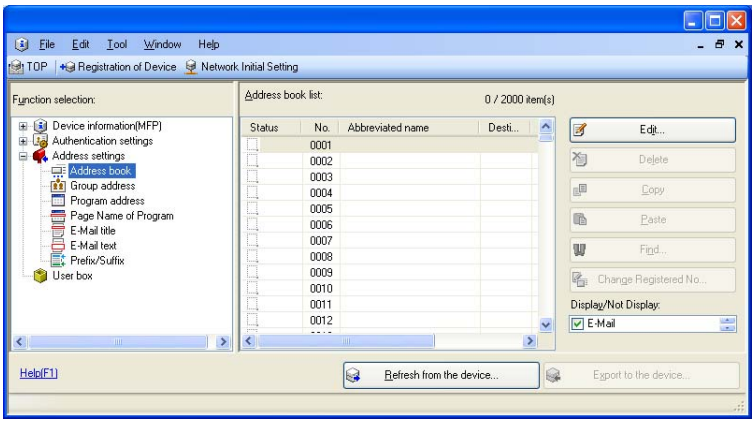
✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

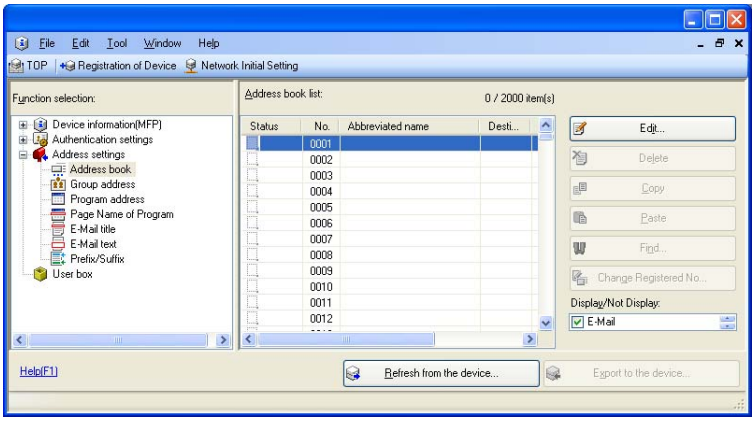
1 Access the machine through [Authentication Settings/Address Settings] mode of PageScope Data Administrator.

2 Click the Address settings expand button.

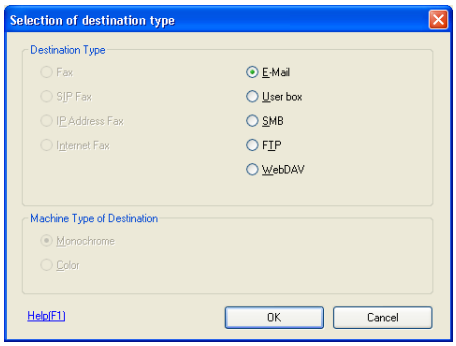
3 Click [Address book].



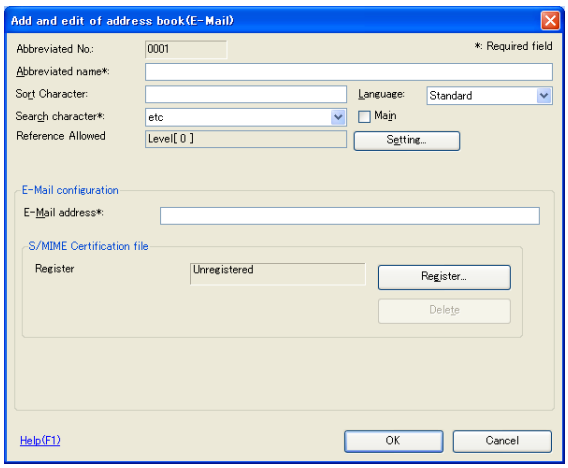
4 Select the number to be registered and click [Edit].



5 Select [E-Mail] and Click [OK].

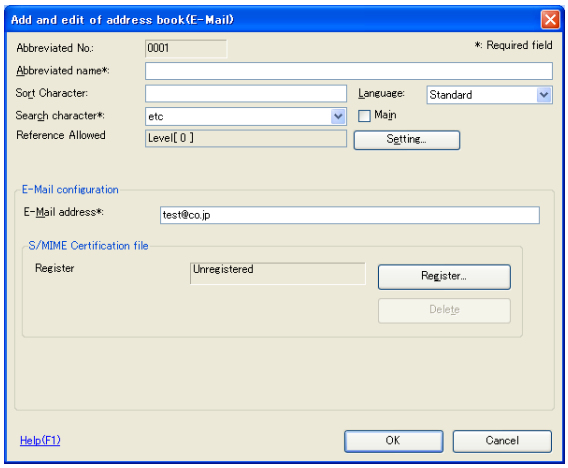


6 Click [Register] of S/MIME Certification file and select the certificate to be registered.



➔ Set 1024 bits or more for the key length of the RSA public key for the certificate of each destination.

7 Make the necessary settings.



➔ If the abbreviated name and E-mail address have not been entered, an input error message appears. Then, click [OK] and enter the abbreviated name and E-mail address.

8 Click [OK].

9 Click [Export to the device].

➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

➔ If there is a job being executed or a reserved job (timer TX, fax redial waiting, etc.) in the machine, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.7 DNS Server Setting Function

<Registering the DNS Server>

✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

1 Access the machine through [Administrator settings] mode of PageScope Data Administrator.

2 Click the Administrator settings expand button.

3 Click the Network expand button.

4 Click [DNS].

5 Make the necessary settings for the DNS Server.

➔ If the DNS Server Auto Obtain and DNS Domain Auto Obtain check boxes are selected, the DNS Server Address and DNS Domain Name are automatically obtained.

6 Click [Export to the device].

➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.8 AppleTalk Setting Function

<Making the AppleTalk Setting>

✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

1 Access the machine through [Administrator settings] mode of PageScope Data Administrator.

2 Click the Administrator settings expand button.

3 Click the Network expand button.

4 Click [AppleTalk].

5 Make the necessary settings.

6 Click [Export to the device].

➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

4.1.9 E-Mail Setting Function

<Setting the SMTP Server (E-Mail Server)>

✔ For the procedure to access the machine, see steps 1 through 5 of page 4-2.

✔ Do not leave the site while you are gaining access to the machine through PageScope Data Administrator. If it is absolutely necessary to leave the site, be sure first to log off from the PageScope Data Administrator.

1 Access the machine through [Administrator settings] mode of PageScope Data Administrator.

2 Click the Administrator settings expand button.

3 Click the Network expand button.

4 Click [E-Mail TX (SMTP)].

5 Make the necessary settings.

6 Click [Export to the device].

➔ If you have already logged on to the Administrator Settings via the control panel or using PageScope Web Connection, the machine displays a message that tells that the write operation has not been successful because of a device lock error. Click [OK] and wait for some while before attempting to execute [Export to the device] again.

KONICA MINOLTA

http://konicaminolta.com

A55V-9607B-00

© 2014 KONICA MINOLTA, INC.